Intrusion SecureNet™ Sensor Appliance User Guide

700-0619-101 Rev C
July 2003

This document covers appliances with Intrusion SecureNet Sensor v4.4 and SecureNet WBI v2.1.

Copyrights

Intrusion SecureNet™ Sensor Appliance User Guide

700-0619-101 Rev C

Intrusion Inc. makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Intrusion Inc. shall not be liable for errors contained herein or for direct, indirect, special, incidental, or consequential damages in connection with the furnishing, performance, or use of this material.

Intrusion Inc. reserves the right to make corrections, updates, or revisions to this information.

IMPORTANT NOTICE

This user document may not be the latest revision available for your Intrusion Inc. product. Upgrades to our documentation, when available, are posted to our internet website at http://www.intrusion.com (arranged by product). Documents are provided in Adobe™ Portable Document Format (PDF) files for download free of charge.

Document upgrades may be replacements of existing documents (revisions), information to be added to existing documents (addenda), or information that corrects errors in existing documents (errata sheets).

Trademarks

Intrusion Inc., SecureNet, and SecureNet Pro are trademarks of Intrusion Inc.
All other products or services mentioned in this document are covered by the trademarks, service marks, or product names as designated by the companies who own or market them.

License Agreement

PLEASE READ CAREFULLY BEFORE CONTINUING WITH THIS INSTALLATION. AT THE END OF THE LICENSE TERMS AND CONDITIONS STATED BELOW, YOU WILL BE ASKED TO ACCEPT OR REJECT SUCH TERMS. BY INDICATING YOUR ACCEPTANCE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT.

This is a legal agreement between the end user (“You”) and Intrusion Inc., its affiliates and subsidiaries (collectively “INTRUSION INC.”). This Agreement may be superseded by any written agreement signed by both You and INTRUSION INC. This Agreement is part of a package (the “Package”) that may also include a sealed CD-ROM disk, sealed diskettes (collectively, the “Disk”) or a downloaded installation package from the INTRUSION INC. web site and certain written materials delivered to You in hard copy or electronic format (the “INTRUSION INC. documentation”).

GRANT OF LICENSE. Subject to the terms and conditions of this License Agreement, INTRUSION INC. grants You a non-exclusive, non-transferable license, to use the following INTRUSION INC. software program (the “SOFTWARE”) in accordance with the instructions contained in the INTRUSION INC. documentation. INTRUSION INC. software can be installed on or assess computers or devices up to the total number of copies authorized for each respective operating system or device. The software for each central monitoring station, “Consoles” and “Managers” can be installed up to the total number of copies authorized for each device.

OWNERSHIP AND COPYRIGHT. Title to the SOFTWARE, including its component parts and user interface, and associated INTRUSION INC. documentation, and patents, copyrights and all other property rights applicable thereto, shall at all times remain solely and exclusively with INTRUSION INC. and its suppliers, and the Customer shall not take any action inconsistent with such title. The SOFTWARE is protected by United States, Canadian and other applicable laws and by international treaty provisions. Therefore, You must treat the SOFTWARE and INTRUSION INC. documentation like any other copyrighted materials except that You may (a) make one copy of the SOFTWARE solely for backup and archival purposes, and (b) make a reasonable number of copies of the INTRUSION INC. documentation for Your internal use only, provided all copyright notices, trademarks and other proprietary rights legends affixed to or contained within the original SOFTWARE and INTRUSION INC. documentation are reproduced on the copies and that they are not removed from the original SOFTWARE or INTRUSION INC. documentation itself. Any rights not expressly granted herein are reserved to INTRUSION INC. and its suppliers.

OTHER RESTRICTIONS. You may not cause or permit disclosure, copy (except as expressly permitted above), rent, license, sublicense, lease, disseminate or otherwise distribute or transfer the SOFTWARE, by any means or in any form, without the prior written consent of INTRUSION INC. You may not use any component part of the SOFTWARE owned by an INTRUSION INC. supplier as a standalone program or in any way independently of the SOFTWARE provided to You by INTRUSION INC. You may not modify, enhance, supplement, create derivative works from, adapt, translate, reverse engineer, decompile, disassemble or otherwise reduce the SOFTWARE to human readable form, except and only to the extent such activity is expressly permitted by applicable law notwithstanding this provision. You shall not remove, obscure or alter INTRUSION INC.'s copyright notices, trademarks, or other proprietary rights legends affixed to or contained within the SOFTWARE.

LIMITED WARRANTY. INTRUSION INC. grants a limited warranty only to You that the SOFTWARE will perform substantially in accordance with the INTRUSION INC. documentation for a period of 90 days from the date of delivery by INTRUSION INC. You may contact INTRUSION INC. regarding support service issues during this 90 day period. INTRUSION INC. does not warrant that the functions or features contained in the SOFTWARE will meet Your requirements or that the operation of the SOFTWARE Media will be uninterrupted or error free. You may enter into a separate support service contract directly with INTRUSION INC. for support issues that may arise following the expiration of the 90 day limited warranty. If You choose not to enter into a separate support service contract, any and all related and subsequent support issues shall be directed to the party from which You purchased this license.

YOU UNDERSTAND THAT, IF YOU PURCHASED THE PACKAGE FROM AN AUTHORIZED RESELLER OF INTRUSION INC., THAT RESELLER IS NOT INTRUSION INC.'S AGENT AND IS NOT AUTHORIZED TO MAKE ANY REPRESENTATIONS, CONDITIONS OR WARRANTIES, STATUTORY OR OTHERWISE, ON INTRUSION INC.'S BEHALF NOR TO VARY ANY OF THE TERMS OR CONDITIONS OF THIS AGREEMENT. IN ADDITION, YOU ACKNOWLEDGE THAT, EXCEPT TO THE EXTENT OTHERWISE AGREED BY THAT RESELLER IN WRITING OR PROHIBITED BY LAW, THE LIMITATIONS OF CONDITIONS AND WARRANTIES, STATUTORY OR OTHERWISE, AND LIABILITY SET FORTH IN THIS AGREEMENT ALSO APPLY TO AND BENEFIT THAT RESELLER.

CUSTOMER REMEDIES. INTRUSION INC.'s entire liability and Your exclusive remedy for breach of the Limited Warranty shall be at INTRUSION INC.'s option, either (a) return of the price paid by You solely for the SOFTWARE, which is returned to INTRUSION INC. and determined by INTRUSION INC. not to be in compliance, or (b) repair and replacement of the SOFTWARE which does not meet INTRUSION INC.'s Limited Warranty. Any replacement SOFTWARE will be warranted for the remainder of the original warranty period or 30 days, whichever is longer. The Limited Warranty is void if failure of the SOFTWARE has resulted from causes other than normal use, including but not limited to, unauthorized repairs, maintenance or modifications to the SOFTWARE, accident, abuse, negligence, misapplication, or failure to use the SOFTWARE in accordance with the INTRUSION INC. documentation. EXCEPT FOR THE FOREGOING EXPRESS CONDITIONS AND WARRANTIES MADE BY INTRUSION INC., INTRUSION INC. AND ITS SUPPLIERS DISCLAIM ALL CONDITIONS, REPRESENTATIONS AND WARRANTIES, STATUTORY OR OTHERWISE, BOTH EXPRESS AND IMPLIED, WITH RESPECT TO THE SOFTWARE, ITS QUALITY AND PERFORMANCE AND THE ACCOMPANYING INTRUSION INC. DOCUMENTATION AND OTHER WRITTEN MATERIALS, INCLUDING BUT NOT LIMITED TO IMPLIED CONDITIONS OR WARRANTIES, STATUTORY OR OTHERWISE, OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied conditions or warranties, statutory or otherwise, so the above exclusion may not apply to You. This warranty gives You specific legal rights, and You may also have other rights which vary from jurisdiction to jurisdiction.

LIMITATION OF LIABILITY. INTRUSION INC. AND ITS SUPPLIERS' LIABILITY WILL BE LIMITED IN ANY EVENT TO ACTUAL DIRECT DAMAGES TO THE EXTENT CAUSED SOLELY BY THE ACTS OR OMISSIONS OF INTRUSION INC., SUBJECT TO A MAXIMUM AGGREGATE LIABILITY FOR ALL CLAIMS OF THE AMOUNT PAID FOR THE SPECIFIC PRODUCT WHICH DIRECTLY CAUSED SUCH DAMAGE. IN NO EVENT SHALL INTRUSION INC. OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, EXEMPLARY, PUNITIVE OR INCIDENTAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGE FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS, DAMAGE OR DESTRUCTION OF DATA, LOSS OF GOOD WILL, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES OR OTHER PECUNIARY LOSS) WHETHER BASED IN CONTRACT, TORT OR PRODUCTS LIABILITY, INCLUDING NEGLIGENCE AND/OR STRICT LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR THE INTRUSION INC. DOCUMENTATION, EVEN IF INTRUSION INC. OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Some jurisdictions do not allow the exclusion or limitation of special, indirect, consequential, exemplary or incidental damages or the limitation of liability to specified amounts, so the above limitation and exclusion may not apply to You.

TERMINATION. INTRUSION INC. shall have the right to terminate this Agreement after giving written notice to You of Your failure to satisfy any of Your obligations hereunder if You then fail to cure such failure to INTRUSION INC.'s satisfaction within thirty (30) days after receiving such notice. In addition, INTRUSION INC. shall have the right to terminate this Agreement in the event You cease to do business or become bankrupt. Upon any such termination: (a) You shall cease all use of all copies of the SOFTWARE and INTRUSION INC. documentation which You received hereunder; and (b) You shall return to INTRUSION INC. all copies of the SOFTWARE and INTRUSION INC. documentation, including any copies or partial copies.

GENERAL. This Agreement constitutes the entire understanding between INTRUSION INC. and You with respect to subject matter hereof. Any change to this Agreement must be in writing, signed by INTRUSION INC. and You. Terms and conditions as set forth in any purchase order which differ from, conflict with, or are not included in this License Agreement, shall not become part of this Agreement unless specifically accepted by INTRUSION INC. in writing. You shall be responsible for and shall pay, and shall reimburse INTRUSION INC. on request if INTRUSION INC. is required to pay, any sales, use, withholding, value added tax (VAT), consumption or other tax (excluding any tax that is based on INTRUSION INC.'s net income), assessment, duty, tariff, or other fee or charge of any kind or nature that is levied or imposed by any governmental authority on the SOFTWARE.

U.S. GOVERNMENT RESTRICTED RIGHTS LEGEND. The Software is provided with RESTRICTED RIGHTS. The Software is a “commercial item” as defined at FAR 2.101, consisting of “commercial computer software” and “commercial computer software documentation” as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DFARS 227.7202, use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in this License Agreement. The contractor/manufacturer is INTRUSION INC., Inc., 1101 East Arapaho, Richardson, TX 75081 U.S.A.

EXPORT AND IMPORT COMPLIANCE. You shall comply with all applicable export and re-export laws, regulations and requirements, as the case may be. You may need an export license or re-export authorization in order to comply with United States law. Receipt of the SOFTWARE may be considered an “import” within the meaning of some countries' laws. INTRUSION INC. has undertaken to comply with various countries' applicable laws and regulations governing the import or use of encryption wherever possible. However, INTRUSION INC. cannot warrant such compliance and hereby specifically disclaims all liability, to the extent permitted under applicable law, for any violation of the laws or regulations of countries other than the United States relating to import or use of the SOFTWARE.

GOVERNING LAW; ARBITRATION. This Agreement shall be governed by, and any arbitration hereunder shall apply, the laws of the State of Texas, U.S.A., excluding (a) its conflicts of laws principles and (b) the United Nations Convention on Contracts for the International Sale of Goods (including, without limitation, the 1974 Convention on the Limitation Period in the International Sale of Goods and the Protocol amending the 1974 Convention, done at Vienna April 11, 1980). Any dispute, controversy or claim arising out of or relating to this Agreement or to a breach hereof, including its interpretation, performance or termination, shall be finally resolved by arbitration. The arbitration shall be conducted by three (3) arbitrators, one to be appointed by INTRUSION INC., one to be appointed by You and a third being nominated by the two arbitrators so selected or, if they cannot agree on a third arbitrator, by the President of the American Arbitration Association (“AAA”). The arbitration shall be conducted in English and in accordance with the commercial arbitration rules of the AAA, which shall administer the arbitration and act as appointing authority. The arbitration, including the rendering of the award, shall take place in Dallas, Texas, and shall be the exclusive forum for resolving such dispute, controversy or claim. The arbitrators' decision shall: (a) be in writing; (b) include reasons for the factual and legal conclusions therein; and (c) shall be consistent with the provisions of Section 5 and Section 6 of this License Agreement. The decision of the arbitrators shall be binding upon the parties thereto, and the expense of the arbitration (including without limitation the award of attorneys' fees to the prevailing party) shall be paid as the arbitrators determine. The decision of the arbitrators shall be executory, and judgment thereon may be entered by any court of competent jurisdiction. Notwithstanding anything contained in this Paragraph 11 to the contrary, INTRUSION INC. shall have the right to institute judicial proceedings against You or anyone acting by, through or under You, in order to enforce INTRUSION INC.'s rights hereunder through reformation of contract, specific performance, injunction or similar equitable relief.

MISCELLANEOUS. Neither this Agreement nor any rights or obligations hereunder may be assigned or delegated (whether by operation of law or otherwise) by You without INTRUSION INC.'s prior written consent. The parties are independent contractors and neither party shall have any right, power or authority to create any obligation or responsibility on behalf of the other. If any provision of this License Agreement is illegal or invalid, such provision shall be changed and interpreted so as to best accomplish the objectives of the original provision to the fullest extent allowed by law and the remaining provisions of this License Agreement shall remain in full force and effect. This License Agreement constitutes the final, complete and exclusive agreement between the parties with respect to the subject matter hereof and supersedes any prior or contemporaneous agreement. No modification, amendment or waiver of any provision of this License Agreement shall be effective unless in writing and signed by the party to be charged.

By accepting this License Agreement, You agree to be bound by such License Terms and Conditions stated above.

If You do not choose to be bound by the above License Terms and Conditions, please contact the party You purchased this license from for refund and return information relating to the non-acceptance of the License Terms and Conditions.

For questions, assistance, or suggestions, contact:

Intrusion Inc. Technical Services Group

Phone	1-888-637-7770
FAX	1-972-234-4059
E-mail	help@intrusion.com
Hours	8:00 AM - 6:00 PM (Central Time Zone)
	Monday through Friday
Address	1101 E. Arapaho Road
	Richardson, Texas 75081
Website	http://www.intrusion.com

Printed in the United States of America.

Contents

Figures

About This Guide

This guide provides information about using the Intrusion SecureNet™ WBI to configure and monitor your SecureNet Sensor appliance. Intrusion SecureNet WBI is a versatile configurable monitoring platform. For you to understand and use Intrusion SecureNet WBI functionality, you must understand the package and its capabilities.

Audience

This user guide provides information necessary to use the Intrusion SecureNet WBI and perform configuration and monitoring of a SecureNet Sensor. This guide is primarily for network and security personnel who configure sensors and monitor networks for evidence of intrusion attempts.

Viewing the Guide

This guide can be read using the Adobe Acrobat Reader. The Adobe *Portable Document Format* (PDF) file displays the Intrusion Inc. user guide in full color and is similar to an online help system. When you view the guide in the Acrobat Reader you can:

- Control the size of the displayed information.
- Print all or a portion of the user guide.
- Find a specific topic using full-text search procedure.
- Use bookmarks and hyperlinks to swiftly navigate among the pages.

Note As you view the Intrusion Inc. documentation online, you will see text that is highlighted as Underscored Blue. This highlight indicates that the associated text is a hyperlink (active link) that "jumps" you to another portion of the document. Hyperlink text is found in the Table of Contents and throughout the text in chapters.

Setting Magnification

To set the magnification for viewing the guide, perform the following steps:

Step 1 Press **[Control]+[M]** keys to display the **Zoom To** dialog box.

Step 2 Type a value for the **Magnification** you want and click on **OK**.

Acrobat displays the guide pages at the specified magnification.

Viewing the Guide with Bookmarks

Step 1 Choose the **Show Bookmarks** command from the **Windows** menu.

The bookmarks display as an interactive table of contents.

Step 2 Click on the Bookmark for the guide section you want to view.

The Bookmark's page and location display in the Acrobat window.

Printing the Guide

Step 1 Choose the **Print** command from the **File** menu or press **[Control]**+**[P]** keys to access the **Print** dialog box.

Step 2 Select the printer and specify the number of copies to print.

Step 3 Type the page numbers (starting and ending) in the **From** and **To** text fields.

Step 4 Click on the **Print** button.

Searching the Guide

To search the guide for a word or string of characters, perform the following steps:

Step 1 Choose **Edit >Find** or press **[Control]**+**[F]** to access the **Find** dialog box.

Step 2 Type the word (or words) to search for in the text field and click on the **Find** button.

Acrobat displays the page on which the first instance of your search string is located.

Step 3 If you want to find the next occurrence of the string, press **[Control]**+**[G]**.

Key Information

This guide uses typeface changes, symbols, and special icons to set apart information in a structured way that makes it easy for the user to read.

Typeface and Symbol Changes

The Intrusion Inc. documents contain procedures that use typeface changes and symbols defined in preface Table 1:

Table 1 What Typeface Changes and Symbols Mean

Typeface or Symbol	Meaning in Paragraph Text or Command Line Example	Examples
italics	Used for: • Document or software titles • Text *new terms* • Words that require emphasis	*Intel PRO/100+ Single Port Installation Guide.* *Network Interface Card* (NIC) You *must* be root user to perform this.
Bold	Denotes *graphical user interface* (GUI) objects. For example, menu titles, button labels, radio buttons, etc.	Click on the **Change Password** button.

Table 1 What Typeface Changes and Symbols Mean- **(Continued)**

Typeface or Symbol	Meaning in Paragraph Text or Command Line Example	Examples
[Alt]+[F]	Keyboard keys are enclosed in square brackets and bold font. If the keys must be pressed simultaneously, a plus sign is used in the text.	Press **[Ctrl]+[Alt]+[Delete]** to log on.
`Bold fixed-width`	Identifies **`user input`** that must be typed exactly as shown.	Type **`cd`** to change the directory.
`Fixed-width`	Identifies `command output`, including error messages.	`File not found.`
Command > Command	The greater than symbol is placed between the Menu and commands that must be selected in sequence as displayed in a graphical user interface.	**File > Menu**

Special Information Icons

This document presents Notes, Important cautions, and Reminders to highlight information of direct importance to you:

Note Highlights special information that is pertinent to the primary discussion. Information contained is important enough to you that it is set off from normal text and called to your attention.

Important! Identifies information that is critical to the operation or procedure and is necessary to prevent loss or corruption of data.

Reminder This symbol means *"Don't forget!"*. You may need to locate some required information or perform a prerequisite procedure before you do this task or you may need to perform another task after you finish this one.

References and Related Documents

Intrusion Inc. provides detailed documentation to help you use your Intrusion SecureNet WBI. Intrusion Inc. documentation is designed to help you find product functionality and step-by-step procedures.

The following documents may provide additional pertinent information:

- *Intrusion PDS Pilot User Guide* available at https://www.intrusion.com/products/downloads/pds_pilot_ug.pdf
- *Intrusion Nexus User Guide* available at https://www.intrusion.com/products/downloads/PDSNexusv1.4UG.pdf
- *Intrusion SecureNet Provider User Guide* available at https://www.intrusion.com/products/downloads/SNProviderv2.1UG.pdf

Intrusion Inc. Contact Information

For answers to your technical support questions or to suggest ways to improve the Intrusion Inc. SecureNet™ product, please contact us at:

Intrusion Inc. Technical Services Group

Phone	1-888-637-7770
Fax	1-972-234-4059
E-mail	help@intrusion.com
Hours	8:00 AM - 6:00 PM (Central Time Zone)
	Monday through Friday
Address	1101 E. Arapaho Road
	Richardson, TX 75081
Support Website	https://serviceweb.intrusion.com

Chapter 1
Overview

This chapter provides an overview of the Intrusion SecureNet Sensor appliance and basic information to help you understand how to use the SecureNet WBI, the web browser interface that you use to monitor and configure the SecureNet Sensor.

Each new SecureNet appliance-based Sensor includes the SecureNet WBI. To ensure that your Sensor appliance has the latest versions of SecureNet Sensor and SecureNet WBI software, refer to Chapter 2 of this user guide for instructions on installing and updating your software.

SecureNet Sensor

The SecureNet Sensor is a network intrusion detection system (NIDS). It analyzes network traffic for events that may indicate that the connections between computers are being exploited and that the data accessible via a network connection is vulnerable to theft, damage, or loss. Based on scanning network traffic for patterns of information packets (defined in signatures), the Sensor can detect a broad range of attacks on corporate information assets, which may include Denial of Service (DoS or DDoS for Distributed-DoS) attacks that attempt to stop the enterprise or its customers from accessing corporate IT assets. The SecureNet Sensor can send an alert identifying the attack, and, in many cases, it can stop attacks before the intruders can access information assets or cause damage. SecureNet Sensors are effective for monitoring both inbound and outbound network traffic.

SecureNet WBI

SecureNet WBI provides secure remote management of the SecureNet Sensor appliance from any location with access to the network. It provides a username/ password-protected secure web connection that prevents unauthorized connections and disclosure of event data.

The SecureNet WBI provides summary level monitoring of the SecureNet Sensor that is refreshed periodically to provide you with the latest events. You can view details of any events in which you are particularly interested and you can delete those of no interest to you.

The SecureNet WBI also lets you perform various configuration tasks to control the SecureNet Sensor appliance. SecureNet WBI supports Microsoft Internet Explorer version 5 or newer.

Chapter 2

Installing/Upgrading SecureNet Appliance Software

This chapter provides information for installing Intrusion SecureNet Sensor with Intrusion SecureNet WBI v2.x software on your Intrusion SecureNet appliance. Regardless of whether your appliance is a new appliance that has never been used or it has been protecting your network for a while, you must perform an installation/configuration procedure to update the software on the appliance and set it up for use.

For New Appliances

Software installation/configuration differs depending on the software that is imaged on your appliance's hard drive when you receive it. You can easily tell what image is installed by looking at the Quick Start that is packaged with the unit.

- If the Quick Start for your appliance calls for setting up your appliance and configuring SecureNet WBI v2.x/SecureNet Sensor software, your appliance is already imaged correctly. Go to "Initially Configure Appliance" on page 2-23.
- If the Quick Start for your appliance calls for staging using Intrusion PDS Pilot, go to "Staging a SecureNet Sensor" on page 2-2.
- If your appliance has a CD reader and you want to install SecureNet WBI v2.x from the software CD, go to "Install from Software CD" on page 2-21.

For In-Operation Appliances

If you are upgrading a SecureNet Sensor that is already in operation, you can install SecureNet WBI v2.x in the following ways:

- If you want to upgrade your appliance to SecureNet WBI using the appliance's update mechanism, go to "Install Using Intrusion PDS Pilot" on page 2-10.
- If you want to use Intrusion Nexus to install Intrusion SecureNet WBI, refer to "Install Intrusion SecureNet WBI using Intrusion Nexus" on page 2-16.
- If your appliance has a CD reader and you want to install SecureNet WBI v2.x from the software CD, go to "Install from Software CD" on page 2-21.

Important! If you want to retain existing SecureNet Sensor configuration information and user data, you must not install SecureNet WBI v2.x using the software CD. Use of the CD for installation deletes everything on your appliance's hard drive before installing SecureNet WBI v2.x.

Staging a SecureNet Sensor

This section provides the procedures for staging your new appliance so that you can easily upgrade it to SecureNet WBI v2.x. Staging the appliance lets you use PDS Pilot to install applications and services.

Important! You need to perform staging only if your SecureNet Sensor appliance is new and it has not been pre-imaged with SecureNet WBI v2.x. If your SecureNet Sensor is new and is pre-imaged with SecureNet WBI v2.x, or if your SecureNet Sensor is already protecting your network, go back to the beginning of this chapter and determine the procedure you need to perform.

Many of the parameters that can be specified during staging of PDS Pilot are available in SecureNet WBI v2.x. To allow quick staging of the appliance, the procedures in this section will skip configuration of some parameters.

Set Up for Staging

To stage the appliance, you must use an external personal computer (PC) running a web browser and log into the appliance's secure website on the pre-defined IP address (10.1.2.2). The PC must have Netscape Navigator 4.0 (or higher) or Microsoft Internet Explorer 4.0 (or higher) installed, and JavaScript must be enabled.

Note The external PC that you connect to the appliance must have its Ethernet port set on the same subnetwork as the appliance's secure website. The secure website is on 10.1.2.2 with a subnet mask of 255.0.0.0, so the external PC's Ethernet port must be on 10.1.2.*x*, where *x* is any digit 0-9, except 2.

To connect the external PC to the appliance, perform the following steps:

Step 1 If necessary, power on the appliance. On hardware that has a Power switch, set the **Power** switch to ON (1). On hardware without a Power switch, unplug the power cord, wait a few seconds, and then plug the power cord back into the power outlet.

Step 2 Connect an Ethernet *crossover cable* to the E1 port on the appliance and to the Ethernet port of the PC running the web browser.

Perform Staging

To stage the appliance using the PDS Pilot, perform the following steps:

Step 1 On the external PC's web browser, enter the following URL:

```
https://10.1.2.2
```

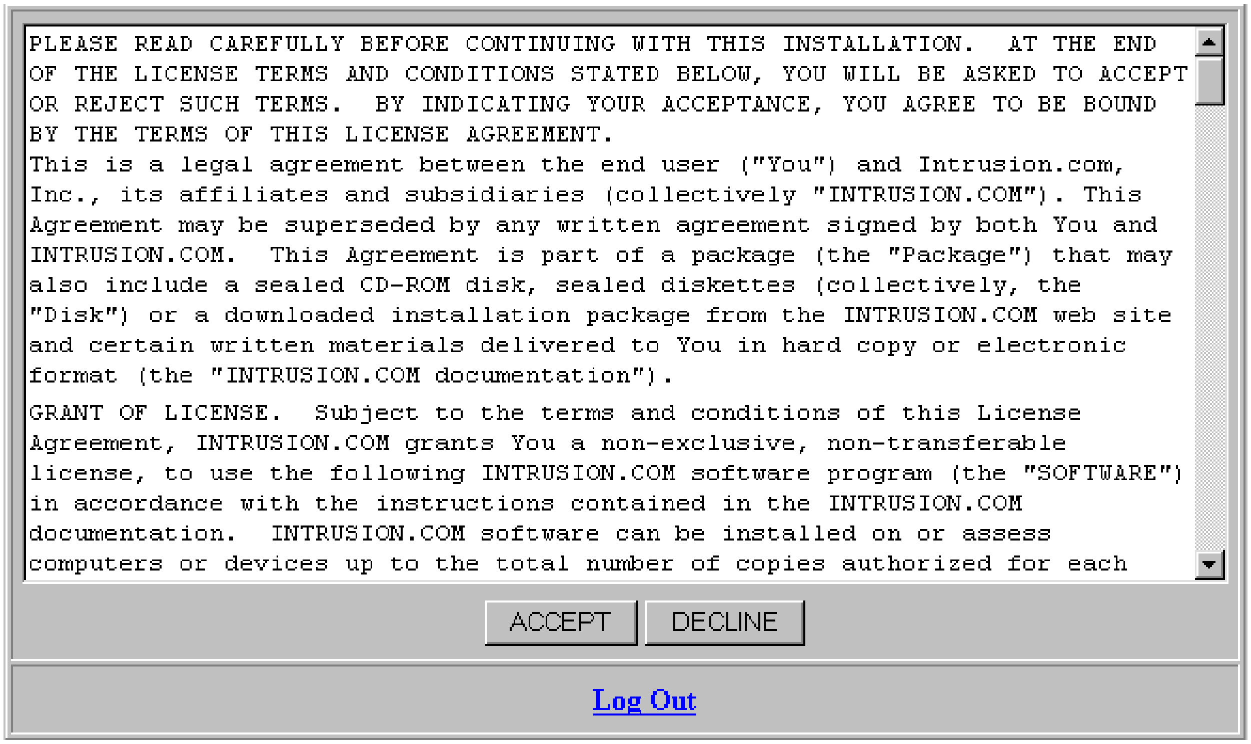
and then press **[Enter]**. A series of new certificate dialogs display. Read and accept each dialog as requested to continue.

The PDS Pilot Login page displays. If you are unable to connect to the PDS Pilot Login page, check that you have correctly connected an operational crossover cable and check that you have set an appropriate address for the PC as described in "Set Up for Staging".

Note Depending on the PDS Pilot version that is imaged on your appliance, the PDS Pilot Login page may have an option to choose PDS Pilot or SecureNet WBI. For this procedure, leave the option in its default state, PDS Pilot.

Step 2 Log in to the appliance using the default username "**`intrusion`**" and the default password "**`password`**", and then click on the **Submit** button.

The Software License Agreement page displays (see Figure 2-1).



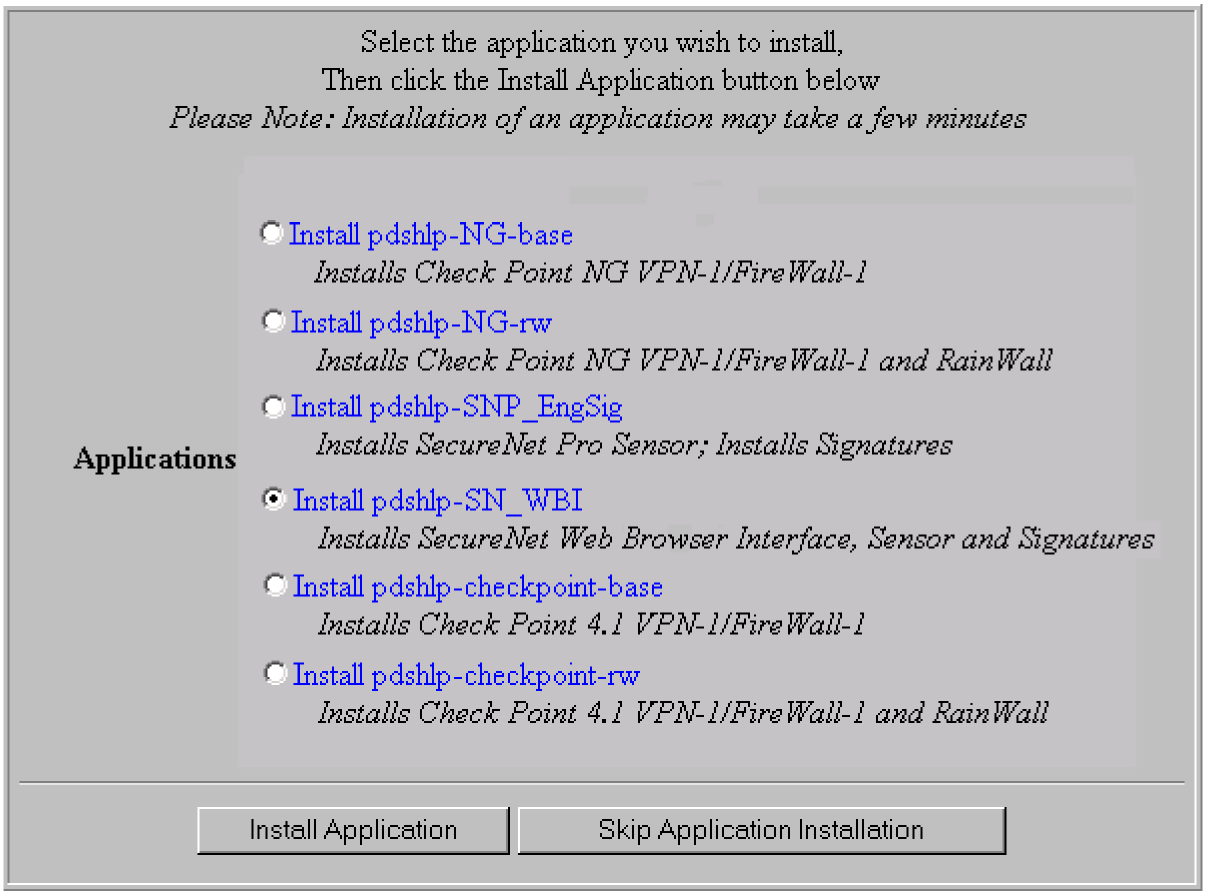
```
PLEASE READ CAREFULLY BEFORE CONTINUING WITH THIS INSTALLATION.  AT THE END
OF THE LICENSE TERMS AND CONDITIONS STATED BELOW, YOU WILL BE ASKED TO ACCEPT
OR REJECT SUCH TERMS.  BY INDICATING YOUR ACCEPTANCE, YOU AGREE TO BE BOUND
BY THE TERMS OF THIS LICENSE AGREEMENT.
This is a legal agreement between the end user ("You") and Intrusion.com,
Inc., its affiliates and subsidiaries (collectively "INTRUSION.COM"). This
Agreement may be superseded by any written agreement signed by both You and
INTRUSION.COM.  This Agreement is part of a package (the "Package") that may
also include a sealed CD-ROM disk, sealed diskettes (collectively, the
"Disk") or a downloaded installation package from the INTRUSION.COM web site
and certain written materials delivered to You in hard copy or electronic
format (the "INTRUSION.COM documentation").
GRANT OF LICENSE.  Subject to the terms and conditions of this License
Agreement, INTRUSION.COM grants You a non-exclusive, non-transferable
license, to use the following INTRUSION.COM software program (the "SOFTWARE")
in accordance with the instructions contained in the INTRUSION.COM
documentation.  INTRUSION.COM software can be installed on or assess
computers or devices up to the total number of copies authorized for each
```

Figure 2-1 Software License Agreement Page

Step 3 Read the software license agreement carefully, and if you agree to the terms specified therein, click on the **ACCEPT** button to continue.

The Application Selection page displays (see Figure 2-2).

Note Figure 2-2 is an example of the Application Selection page. The applications shown on the page vary by appliance.



Select the application you wish to install,
Then click the Install Application button below
Please Note: Installation of an application may take a few minutes

Applications

○ Install pdshlp-NG-base
Installs Check Point NG VPN-1/FireWall-1

○ Install pdshlp-NG-rw
Installs Check Point NG VPN-1/FireWall-1 and RainWall

○ Install pdshlp-SNP_EngSig
Installs SecureNet Pro Sensor; Installs Signatures

● Install pdshlp-SN_WBI
Installs SecureNet Web Browser Interface, Sensor and Signatures

○ Install pdshlp-checkpoint-base
Installs Check Point 4.1 VPN-1/FireWall-1

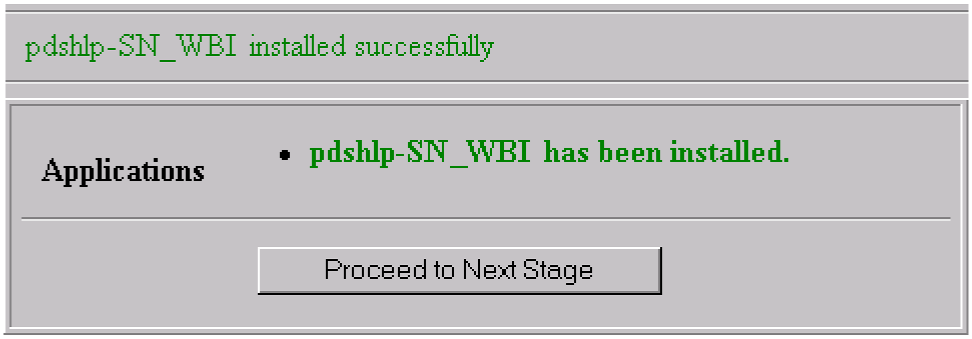
○ Install pdshlp-checkpoint-rw
Installs Check Point 4.1 VPN-1/FireWall-1 and RainWall

Figure 2-2 Application Selection Page

Step 4 Click on the **`Install pdshlp-SN_WBI`** radio button (not the **`Install pdshlp-SNP_EngSig`** button) and then click on **`Install Application`**.

Step 5 Wait for the application to install. Installation may take a few minutes.

When the installation is complete, the Application Selection page redisplays with a message that indicates your selected application is installed. Figure 2-3 shows a successful result message for the installation.



pdshlp-SN_WBI installed successfully

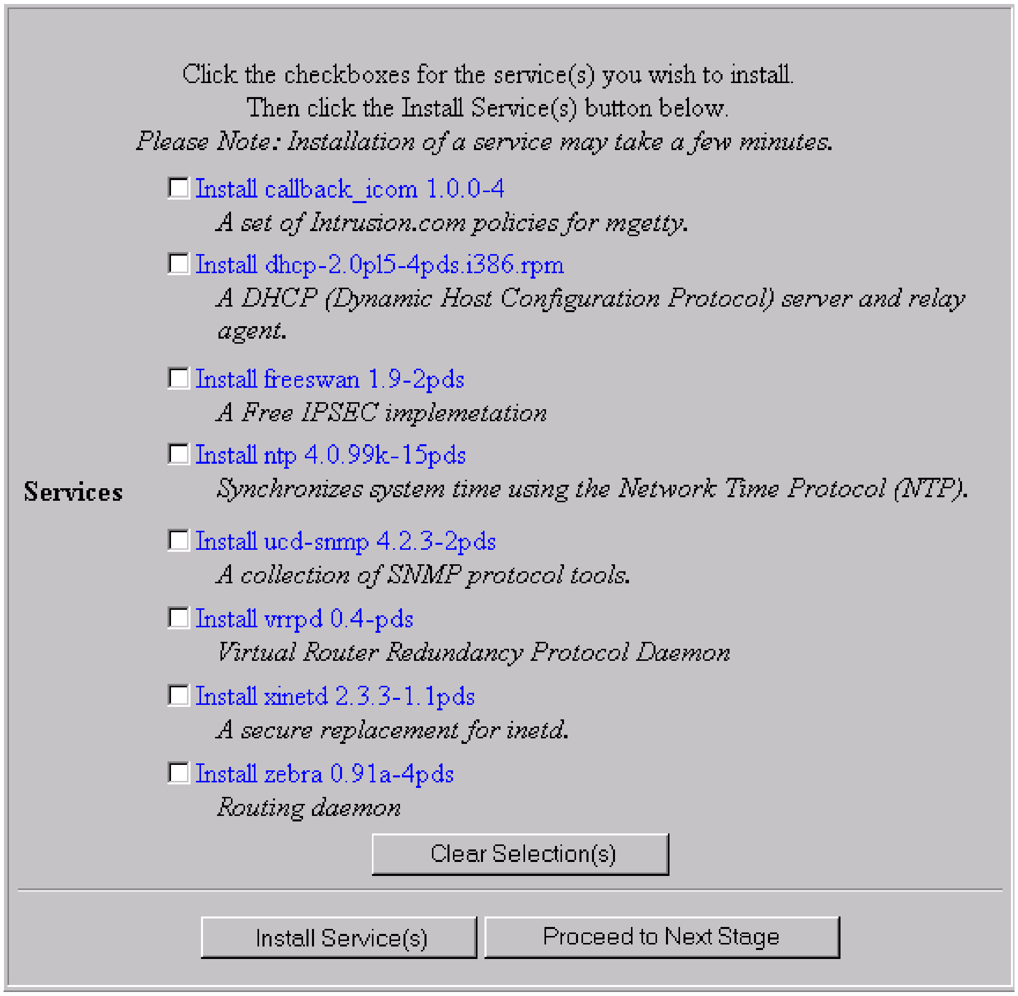
Applications

- **pdshlp-SN_WBI has been installed.**

Figure 2-3 Application Installation Results Page

Step 6 Click on the **Proceed to Next Stage** button.

The Services Selection page displays (see Figure 2-4).



Click the checkboxes for the service(s) you wish to install.
Then click the Install Service(s) button below.
Please Note: Installation of a service may take a few minutes.

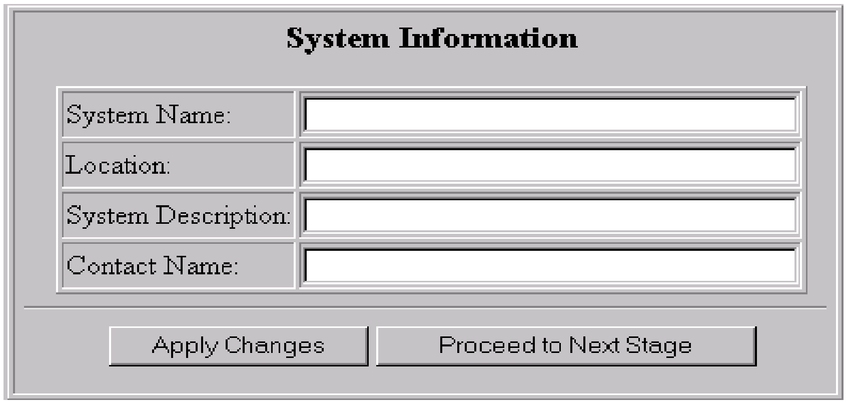
Services

- □ Install callback_icom 1.0.0-4
  A set of Intrusion.com policies for mgetty.
- □ Install dhcp-2.0pl5-4pds.i386.rpm
  A DHCP (Dynamic Host Configuration Protocol) server and relay agent.
- □ Install freeswan 1.9-2pds
  A Free IPSEC implemetation
- □ Install ntp 4.0.99k-15pds
  Synchronizes system time using the Network Time Protocol (NTP).
- □ Install ucd-snmp 4.2.3-2pds
  A collection of SNMP protocol tools.
- □ Install vrrpd 0.4-pds
  Virtual Router Redundancy Protocol Daemon
- □ Install xinetd 2.3.3-1.1pds
  A secure replacement for inetd.
- □ Install zebra 0.91a-4pds
  Routing daemon

Figure 2-4 Services Selection Page

Step 7 Do not select any services. Click on the **Proceed to Next Stage** button. A confirmation message displays confirming that you want to skip installing a service. Click on **OK** to confirm acceptance.

The System Information page shown in Figure 2-5 displays.

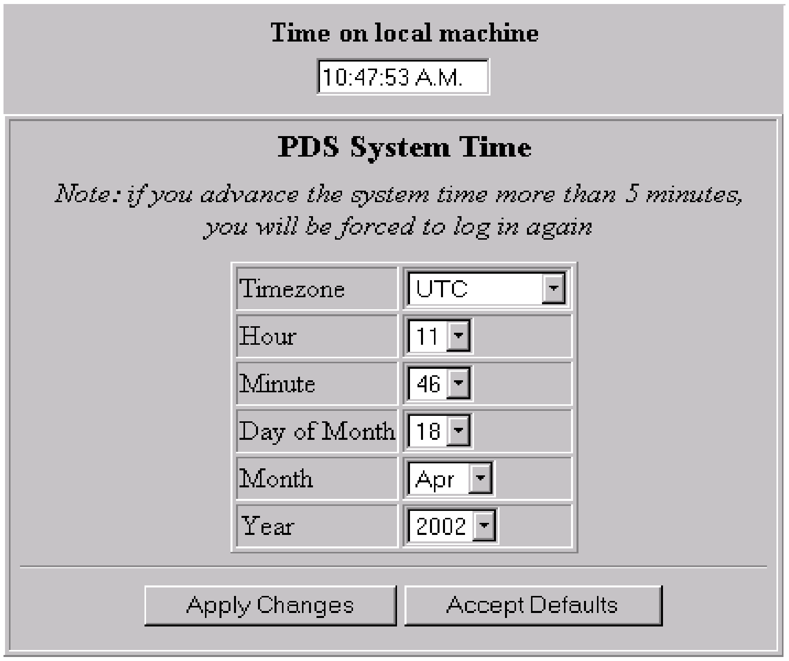

System Information

System Name:	
Location:	
System Description:	
Contact Name:	

Figure 2-5 System Information Page

Step 8 Leave all fields blank and click on the **Proceed to Next Stage** button. A confirmation message displays confirming that you want to skip setting system information. Click on **OK** to confirm acceptance.

The System Time page shown in Figure 2-6 displays.


Time on local machine

10:47:53 A.M.

PDS System Time

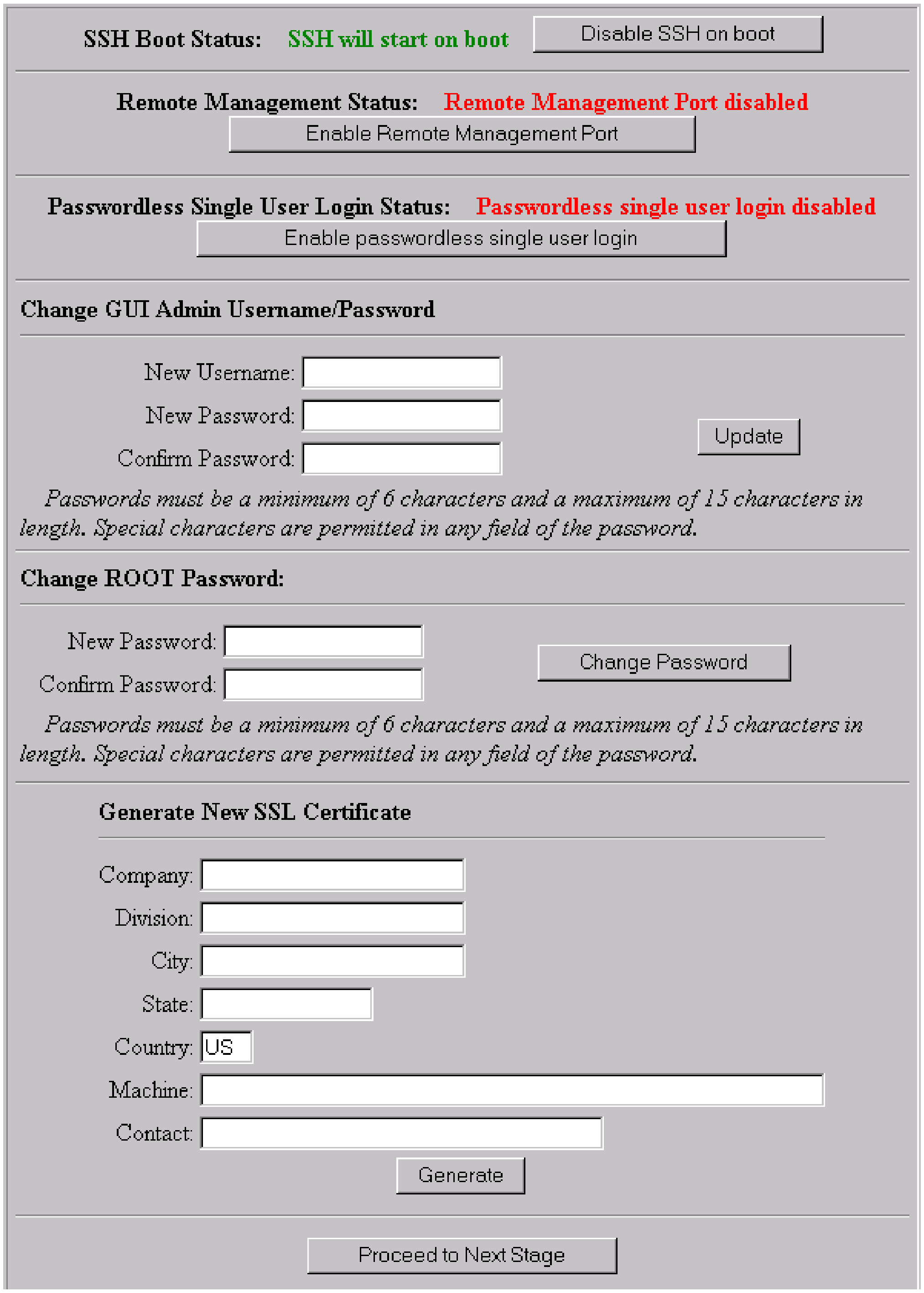
Note: if you advance the system time more than 5 minutes, you will be forced to log in again

Timezone	UTC
Hour	11
Minute	46
Day of Month	18
Month	Apr
Year	2002

Figure 2-6 System Time Page

Step 9 Click on the **Accept Defaults** button to continue. A confirmation message displays confirming that you want to skip changing the system time. Click on **OK** to confirm acceptance.

The Initial Security page displays (see Figure 2-7).



SSH Boot Status: SSH will start on boot

Remote Management Status: Remote Management Port disabled

Passwordless Single User Login Status: Passwordless single user login disabled

Change GUI Admin Username/Password

New Username:

New Password:

Confirm Password:

Passwords must be a minimum of 6 characters and a maximum of 15 characters in length. Special characters are permitted in any field of the password.

Change ROOT Password:

New Password:

Confirm Password:

Passwords must be a minimum of 6 characters and a maximum of 15 characters in length. Special characters are permitted in any field of the password.

Generate New SSL Certificate

Company:

Division:

City:

State:

Country: US

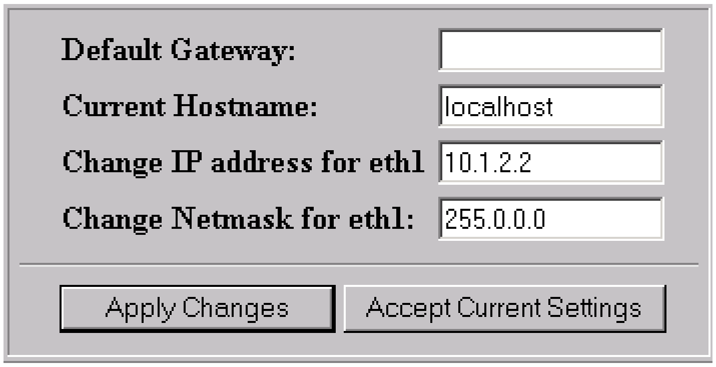
Machine:

Contact:

Figure 2-7 Initial Security Page

Step 10 Leave all fields blank and click on the **Proceed to Next Stage** button.

The Initial Network Settings page displays (see Figure 2-8).



Default Gateway:

Current Hostname: localhost

Change IP address for eth1 10.1.2.2

Change Netmask for eth1: 255.0.0.0

Figure 2-8 Initial Network Settings Page

Step 11 Leave all fields blank and click on the **Accept Current Settings** button.

Step 12 Change the initial network settings fields as needed.

a. In the **Default Gateway** field, type the hostname or IP address (in *dotted quad format*) of the default gateway for the appliance.

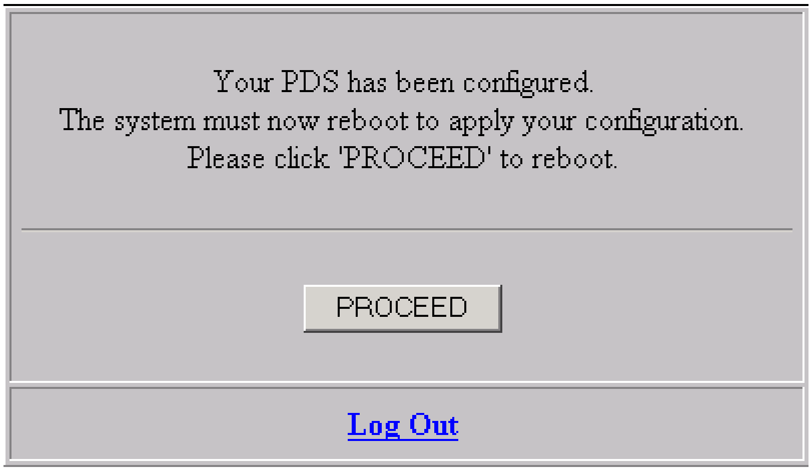
b. In the **Current Hostname** field, type a unique hostname that you want to assign to the appliance.

c. In the **Change IP Address for eth1** field, type the new IP address for the appliance in *dotted quad format*.

d. In the **Change Netmask for eth1** field, type the new netmask for the appliance in *dotted quad format*.

Step 13 Click on the **Apply Changes** button.

The Staging Complete page displays (see Figure 2-9).

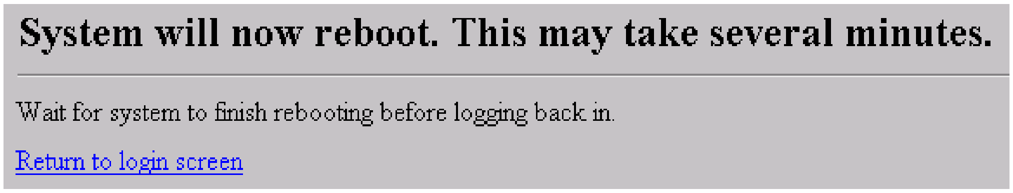


Your PDS has been configured.
The system must now reboot to apply your configuration.
Please click 'PROCEED' to reboot.

Figure 2-9 Staging Complete Page

Step 14 Click on the **PROCEED** button to acknowledge the completion of staging.

The system reboots and the Reboot message shown in Figure 2-10 displays.



System will now reboot. This may take several minutes.

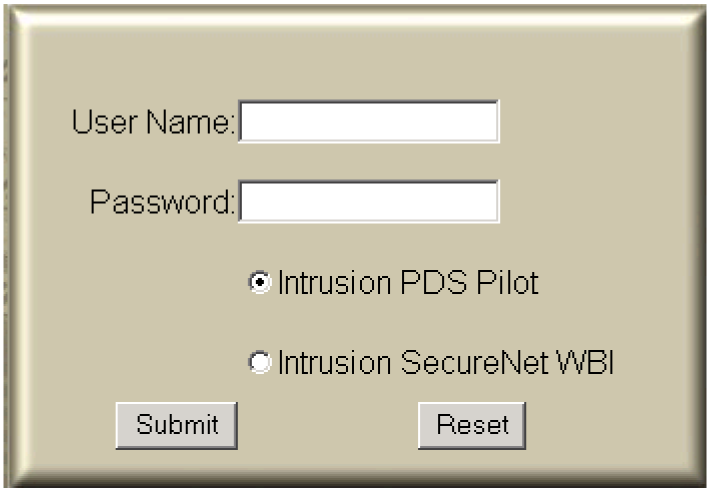
Wait for system to finish rebooting before logging back in.

Return to login screen

Figure 2-10 Reboot Message

Step 15 Wait for the system to reboot and then click on the **Return to login screen** link.

The Intrusion PDS Pilot/SecureNet WBI Login page displays (see Figure 2-11).



User Name:

Password:

● Intrusion PDS Pilot

○ Intrusion SecureNet WBI

Figure 2-11 Intrusion PDS Pilot/SecureNet WBI Login Page

Step 16 Go to "Install Using Intrusion PDS Pilot" on page 2-10 to complete the installation of SecureNet WBI v2.x.

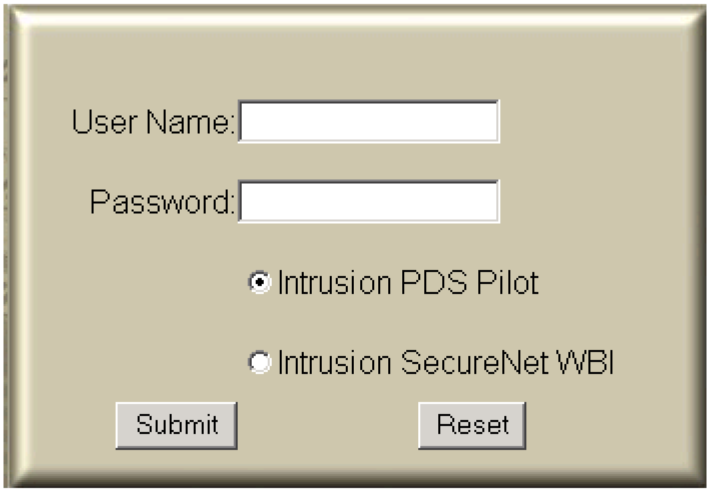
Install Using Intrusion PDS Pilot

To install Intrusion SecureNet WBI v2.x on an appliance that has Intrusion PDS Pilot installed, perform the following steps:

Step 1 If you have just completed the staging of a new appliance using the procedure provided in this chapter, skip to Step 3 on page 2-10. Otherwise, go to Step 2.

Step 2 On a Microsoft Internet Explorer web browser (version 5 or greater), enter the URL assigned to the Ethernet port *eth1* on your Sensor (**`https://<ipaddress>`**) and then press **[Enter]**.

The Intrusion PDS Pilot/SecureNet WBI Login page displays (see Figure 2-12).


User Name:

Password:

● Intrusion PDS Pilot

○ Intrusion SecureNet WBI

Figure 2-12 Intrusion PDS Pilot/SecureNet WBI Login Page

Important! If the login page does not have the PDS Pilot and SecureNet WBI radio buttons as shown in Figure 2-12, you will need to upgrade PDS Pilot to the latest release. You can perform the PDS Pilot upgrade using this procedure, and then repeat the procedure to install SecureNet WBI v2.x.

Step 3 If the login page has the PDS Pilot and SecureNet WBI radio buttons as shown in Figure 2-12, leave **Intrusion PDS Pilot** as the selection.

Note In the following step, if you have just completed staging of a new appliance using the procedure provided in this chapter, use the default username "**`intrusion`**" and the default password "**`password`**") to log in.

Step 4 Enter your administrator username and password, and then click on the **Submit** button.

The Intrusion PDS Pilot Main page displays (see Figure 2-13).

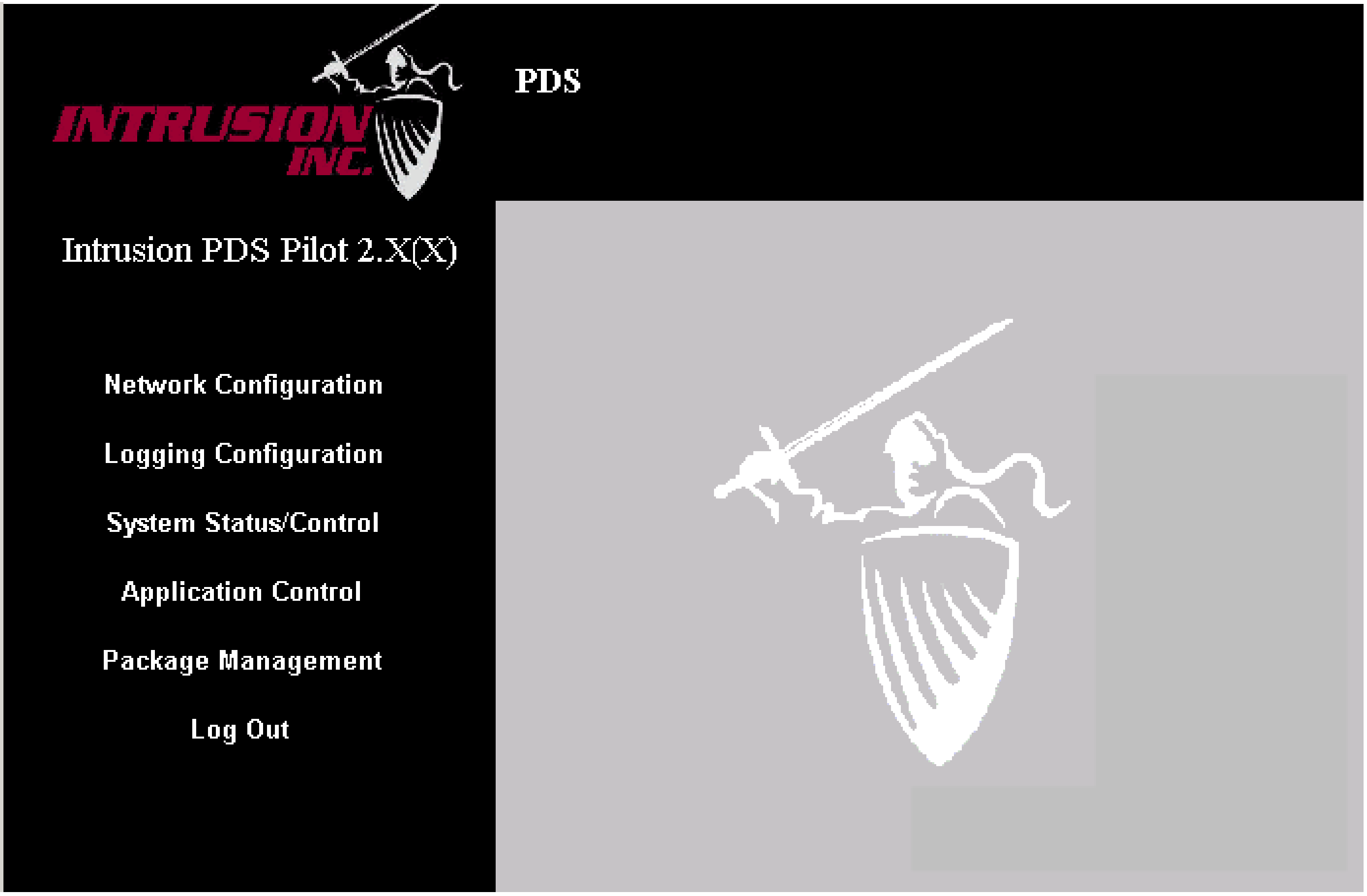
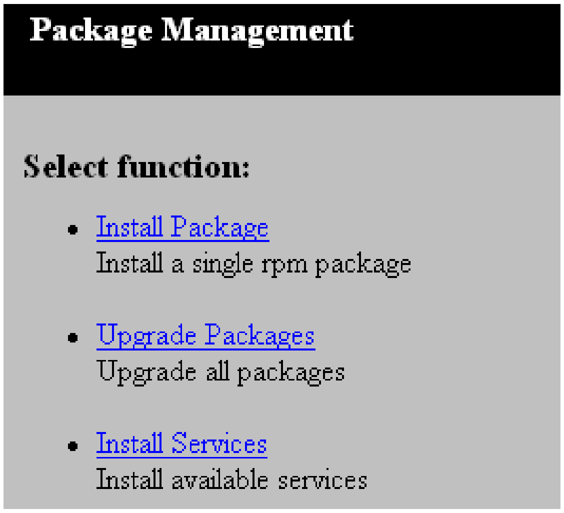


Figure 2-13 Intrusion PDS Pilot Main Page

Step 5 In the Navigation bar on the left side of the page, click on **Package Management**.

The Package Management page displays (see Figure 2-14).



Package Management

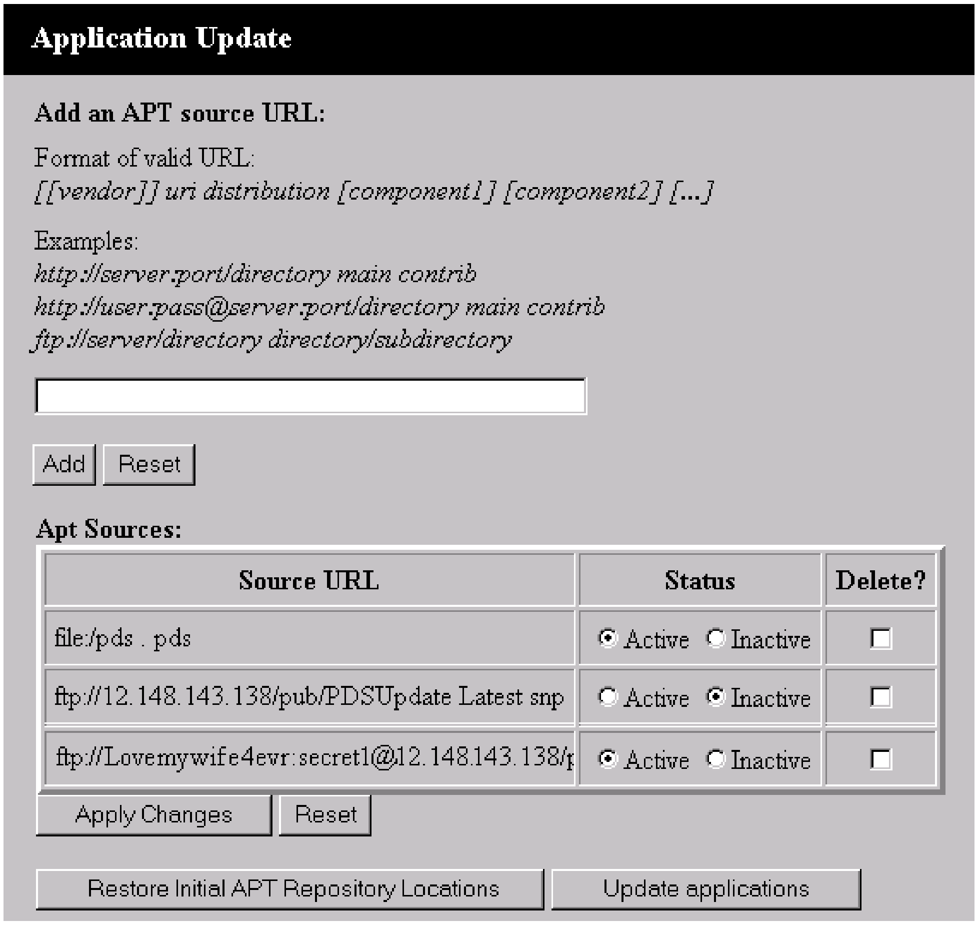
Select function:

- Install Package
  Install a single rpm package
- Upgrade Packages
  Upgrade all packages
- Install Services
  Install available services

Figure 2-14 Package Management Page

Step 6 Click on the **Upgrade Packages** link.

The Application Update page displays (see Figure 2-15).



Application Update

Add an APT source URL:

Format of valid URL:
[[vendor]] uri distribution [component1] [component2] [...]

Examples:
http://server:port/directory main contrib
http://user:pass@server:port/directory main contrib
ftp://server/directory directory/subdirectory

Apt Sources:

Source URL	Status	Delete?
file:/pds . pds	● Active ○ Inactive	□
ftp://12.148.143.138/pub/PDSUpdate Latest snp	○ Active ● Inactive	□
ftp://Lovemywife4evr:secret1@12.148.143.138/p	● Active ○ Inactive	□

Figure 2-15 Application Update Page

Important! Disregard the example URLs shown on the Application Update page (see Figure 2-15). Intrusion's downloadable software files are now available from ServiceWeb, a members-only FTP site reserved for customers who have maintenance agreements with Intrusion Inc. If you do not have a membership, you must go to https://serviceweb.intrusion.com/request.asp to complete and submit an Access Authorization Request form.

When your Access Authorization Request is approved, emails will be sent to the addresses you provided for the Primary Contact and the Secondary Contact. You can then use your ServiceWeb Username and Password when performing software upgrades as described in this procedure.

When you perform an update, PDS Pilot updates RPMs using all the *activated* APT sources in the list. If an RPM is present in two or more places, PDS Pilot gets the RPM with the highest release number (latest version).

Note In the following step, if you are using this procedure to upgrade PDS Pilot to the latest release before installing SecureNet WBI v2.x, you must use the following address:

ftp://<*yourusername*>:<*yourpassword*>@12.148.143.138/pub/PDSUpdate Latest snp
(Be sure to enter the spaces before and after the word “Latest”.)

Step 7 In the **Add an APT source URL** field, type

ftp://<*yourusername*>:<*yourpassword*>@12.148.143.138/pub/PDSUpdate Latest snp
(Be sure to enter the spaces before and after the word “Latest”.)

Step 8 Click on the **Add** button.

The new source is added to the Apt Sources table at the bottom of the page.

Step 9 Click on the **Update applications** button.

The installation completes. The appliance reboots.

Note After the installation completes, the error message “Page Not Found” displays in the browser window. This is normal.

Step 10 Wait a few seconds, and then click on the browser’s **Refresh** button.

The SecureNet WBI Login page displays. If you are using this procedure to upgrade PDS Pilot to the latest release before installing SecureNet WBI v2.x, the login page looks like the one in Figure 2-12. In this case, go to Step 4 on page 2-10.

-OR-

If you are installing SecureNet WBI v2.x, the login page looks like Figure 2-16.

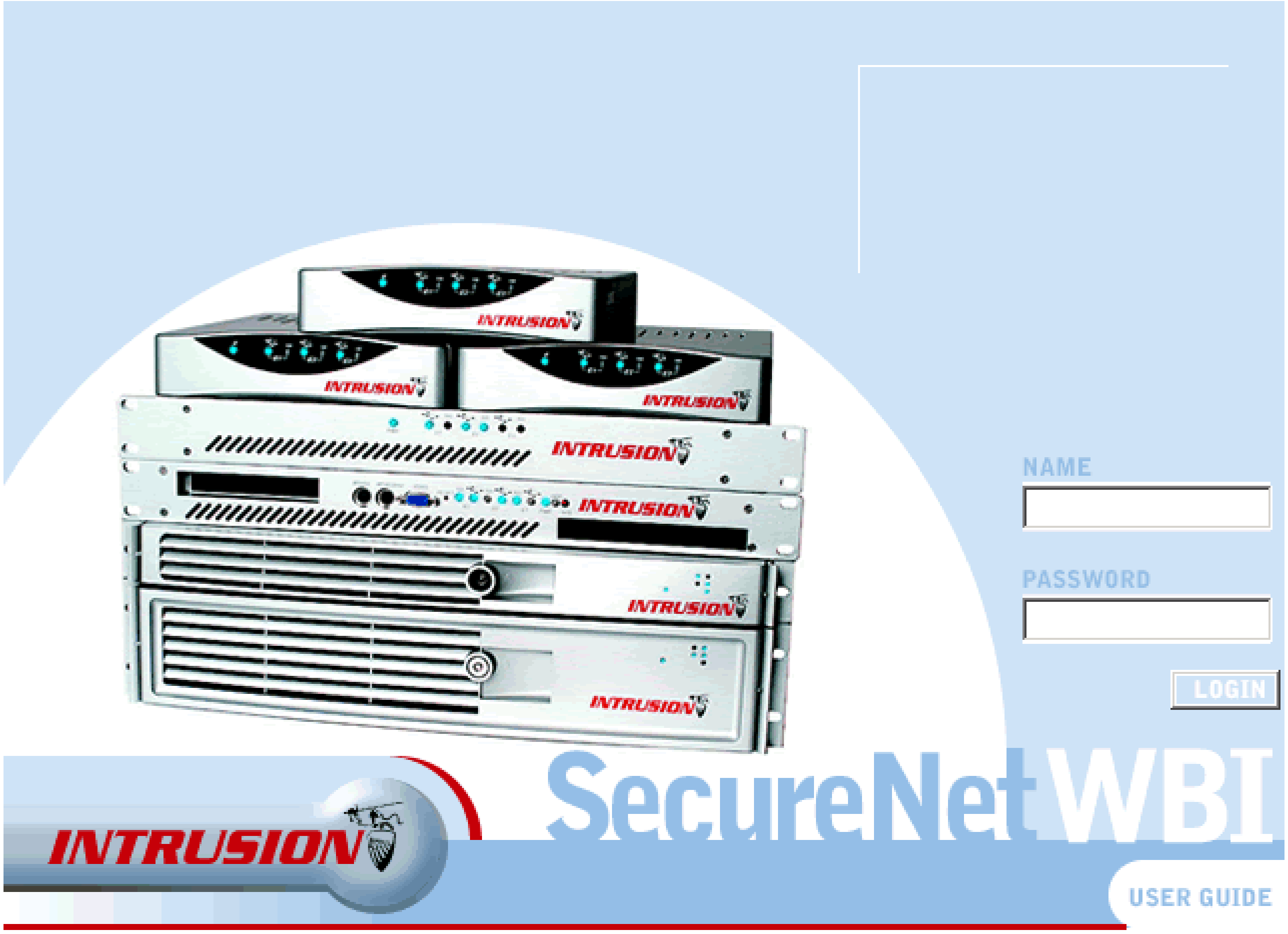


Figure 2-16 SecureNet WBI Login Page

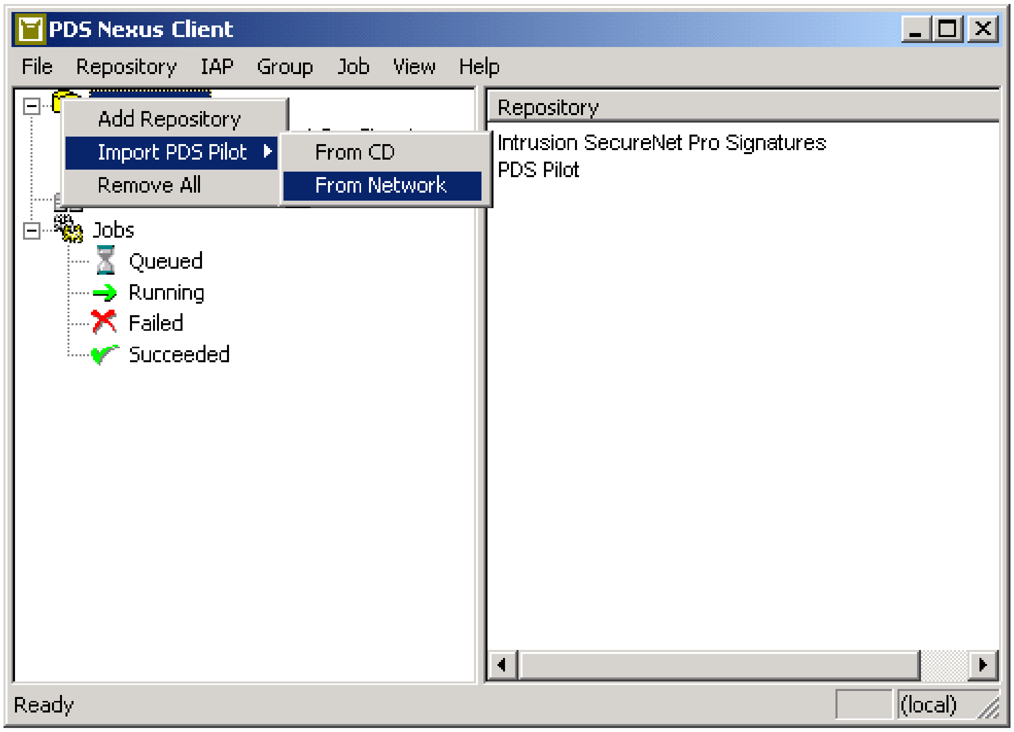
Installation is complete.

Install Intrusion SecureNet WBI using Intrusion Nexus

To use Intrusion Nexus 1.4 to install Intrusion SecureNet WBI on an Intrusion Appliance (IAP), perform the following steps:

Step 1 On the Nexus Client window, right-click on the top-level Repositories icon in the tree pane.

The Repositories context-sensitive menu displays (see Figure 2-17).

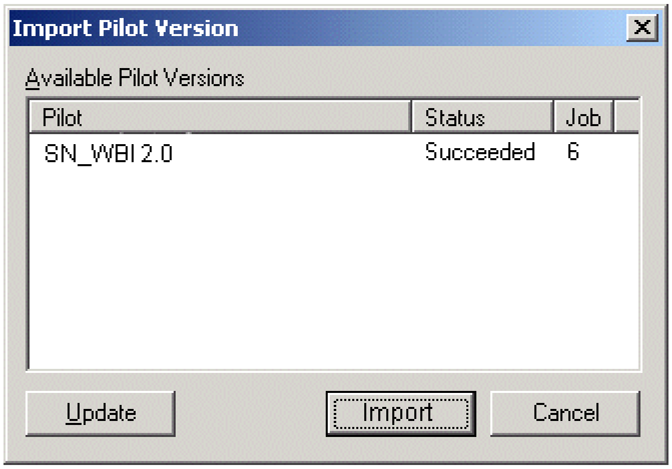


Repository
Intrusion SecureNet Pro Signatures
PDS Pilot

Figure 2-17 Repositories Context-Sensitive Menu - Import Pilot Options

Step 2 Click on **Import PDS Pilot** and then slide to the right and click on **From Network** as the source of the Intrusion PDS Pilot repository.

The Import Pilot Version dialog displays (see Figure 2-18).



Pilot	Status	Job
SN_WBI 2.0	Succeeded	6

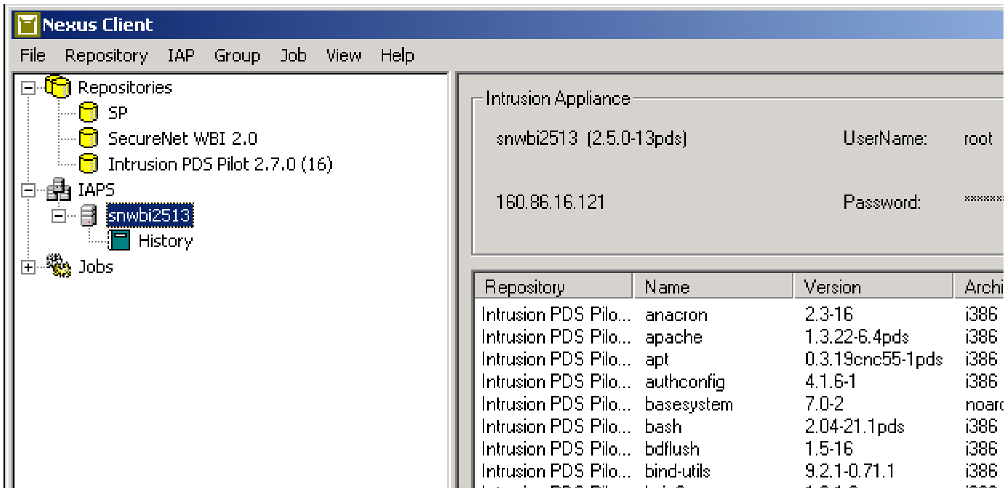
Figure 2-18 Import Pilot Version Dialog

Step 3 Click on **SN_WBI 2.x** to select it and then click on the **Import** button.

The software package is added to the Repository container.

Step 4 View the IAP on which you intend to install Intrusion SecureNet WBI by expanding the IAPS tree pane or IAP Group in which it is contained and then clicking on the IAP.

The IAP's properties display in the details pane (see Figure 2-19).



snwbi2513 (2.5.0-13pds) UserName: root

160.86.16.121 Password: *******

Repository	Name	Version	Archi
Intrusion PDS Pilo...	anacron	2.3-16	i386
Intrusion PDS Pilo...	apache	1.3.22-6.4pds	i386
Intrusion PDS Pilo...	apt	0.3.19cnc55-1pds	i386
Intrusion PDS Pilo...	authconfig	4.1.6-1	i386
Intrusion PDS Pilo...	basesystem	7.0-2	noarc
Intrusion PDS Pilo...	bash	2.04-21.1pds	i386
Intrusion PDS Pilo...	bdflush	1.5-16	i386
Intrusion PDS Pilo...	bind-utils	9.2.1-0.71.1	i386

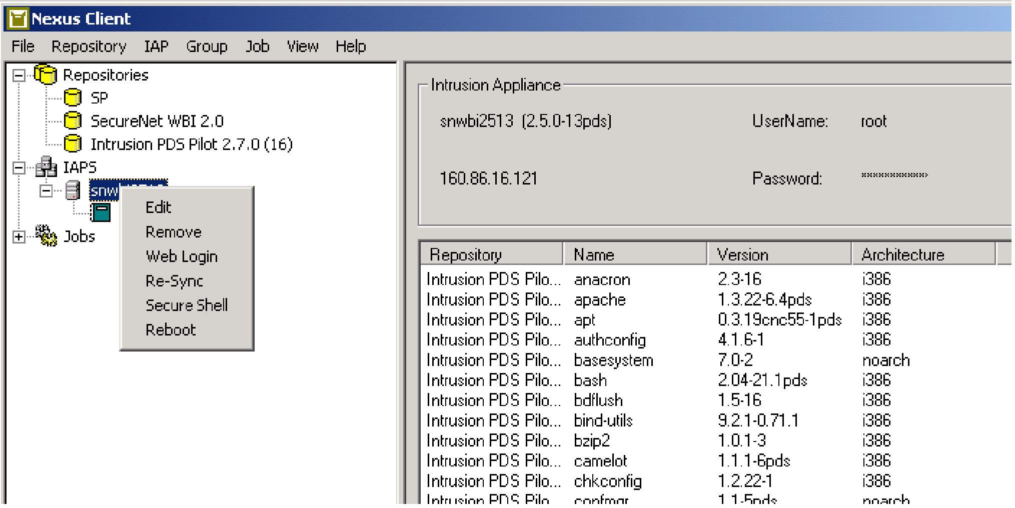
Figure 2-19 View IAP Properties

Step 5 Make sure the target IAP's Intrusion PDS Pilot has been upgraded to at least version 2.4.

If the IAP's Intrusion PDS Pilot version is not at least 2.4, upgrade it to at least version 2.5 before proceeding. Refer to the *Intrusion Nexus User Guide* for more information.

Step 6 Right-click on the IAP on which you intend to install Intrusion SecureNet WBI.

A context-sensitive menu displays (see Figure 2-20).



snwbi2513 (2.5.0-13pds) UserName: root

160.86.16.121 Password: ************

Repository	Name	Version	Architecture
Intrusion PDS Pilo...	anacron	2.3-16	i386
Intrusion PDS Pilo...	apache	1.3.22-6.4pds	i386
Intrusion PDS Pilo...	apt	0.3.19cnc55-1pds	i386
Intrusion PDS Pilo...	authconfig	4.1.6-1	i386
Intrusion PDS Pilo...	basesystem	7.0-2	noarch
Intrusion PDS Pilo...	bash	2.04-21.1pds	i386
Intrusion PDS Pilo...	bdflush	1.5-16	i386
Intrusion PDS Pilo...	bind-utils	9.2.1-0.71.1	i386
Intrusion PDS Pilo...	bzip2	1.0.1-3	i386
Intrusion PDS Pilo...	camelot	1.1.1-6pds	i386
Intrusion PDS Pilo...	chkconfig	1.2.22-1	i386
Intrusion PDS Pilo...	confmgr	1.1-5pds	noarch

Figure 2-20 IAP Context-Sensitive Menu

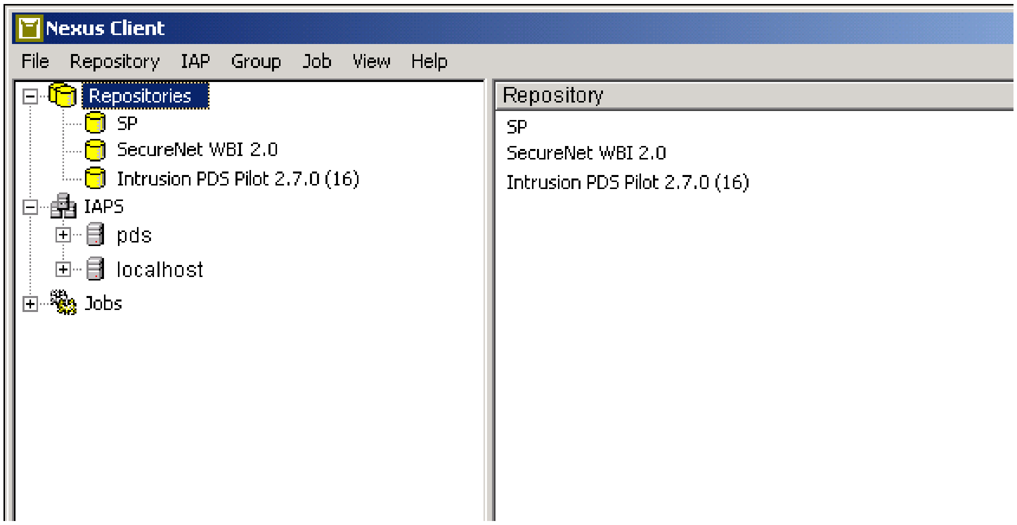
Step 7 Click on **Resync**.

Intrusion Nexus begins resynchronization with the selected IAP.

Step 8 Wait for the resynchronization to complete. It may take several minutes.

Step 9 Click on the top-level Repositories node.

The Repositories node is expanded and the right pane displays the repositories (see Figure 2-21).

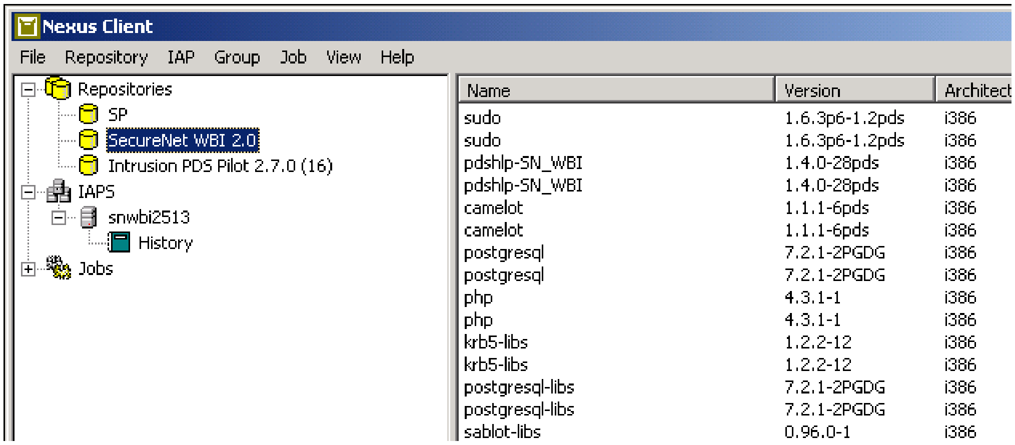


Repository
SP
SecureNet WBI 2.0
Intrusion PDS Pilot 2.7.0 (16)

Figure 2-21 Repositories Node Expanded

Step 10 Click on the **SecureNet WBI 2.x** repository.

The right pane of the window displays the packages in the repository (see Figure 2-22).



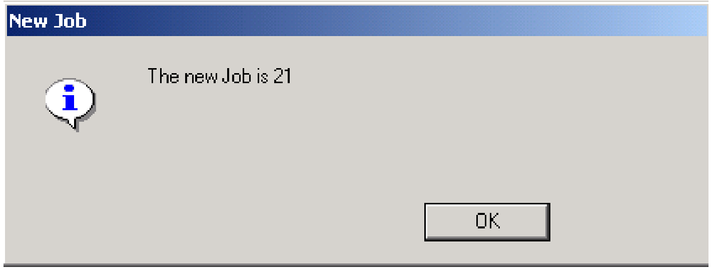
Name	Version	Architect
sudo	1.6.3p6-1.2pds	i386
sudo	1.6.3p6-1.2pds	i386
pdshlp-SN_WBI	1.4.0-28pds	i386
pdshlp-SN_WBI	1.4.0-28pds	i386
camelot	1.1.1-6pds	i386
camelot	1.1.1-6pds	i386
postgresql	7.2.1-2PGDG	i386
postgresql	7.2.1-2PGDG	i386
php	4.3.1-1	i386
php	4.3.1-1	i386
krb5-libs	1.2.2-12	i386
krb5-libs	1.2.2-12	i386
postgresql-libs	7.2.1-2PGDG	i386
postgresql-libs	7.2.1-2PGDG	i386
sablot-libs	0.96.0-1	i386

Figure 2-22 Intrusion SecureNet WBI Repository Expanded

Step 11 Expand the IAPS node to show the target IAP.

Step 12 Use your mouse to drag and drop the **SecureNet WBI 2.x** repository to the target IAP.

The package is queued for distribution to the IAP. Intrusion PDS Nexus responds with a message box telling you what the job number is for this distribution (see Figure 2-23).



The new Job is 21

Figure 2-23 Job Number Confirmation Message

Step 13 Make note of the Job number.

Step 14 Wait for the job to complete. Check the Jobs logs for success or failure of the distribution.

Step 15 Wait for the system to reboot (it may actually take several minutes).

After the IAP reboots, Intrusion SecureNet WBI 2.x is installed and ready for use.

Step 16 Right-click on the IAP.

A pop-up menu displays.

Step 17 Click on **Web Login**.

The Intrusion SecureNet WBI Login page displays (see Figure 2-24.

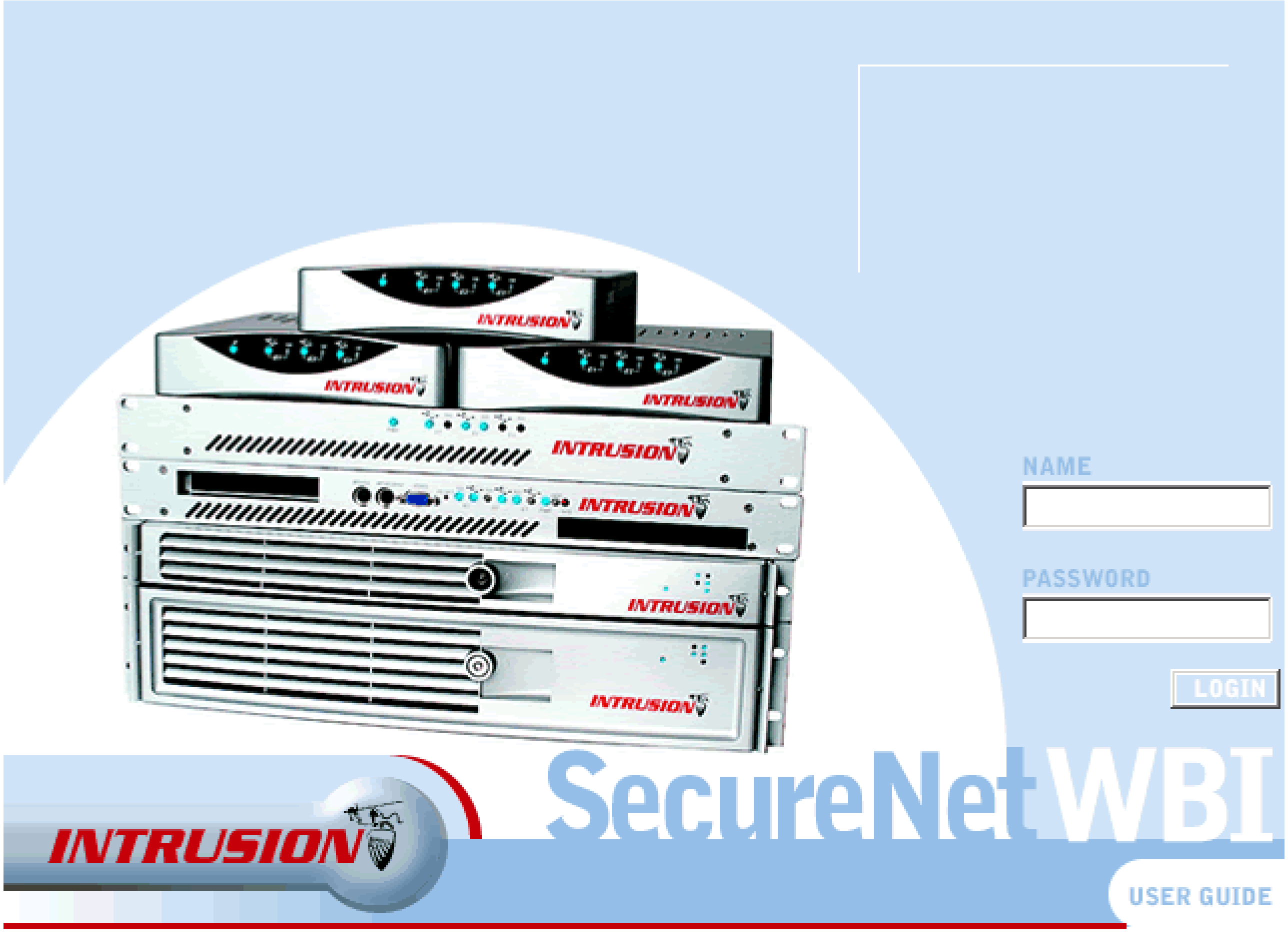


Figure 2-24 SecureNet WBI Login Page

SecureNet WBI 2.x installation on the IAP is complete.

Install from Software CD

This method is available only for SecureNet Sensor appliances that have a CD reader. SecureNet Sensor appliances that have CD readers are set up to boot from the CD reader (that is, the CD reader is defined as a boot disk).

Important! Installing SecureNet WBI v2.x from CD completely removes all existing software, configuration information, and user data from the appliance's storage media. If you are upgrading an existing SecureNet Sensor and want to retain configuration information and user data, do not use this method.

To install SecureNet WBI v2.x from the software CD, perform the following steps:

Step 1 If necessary, physically install your appliance:

a. Mount the appliance in an equipment rack or place it on a suitable flat surface.

b. Set up the appliance connection for "command line interface" (CLI) and display. If necessary, connect a dumb terminal or a terminal emulator to the serial port on the appliance
-OR-
Connect a PS/2 keyboard and a video monitor to the ports on the appliance.

c. Plug the power cord into socket on the rear of the appliance and into an approved power source.

d. Set the **Power** switch to ON (1) and verify that the appliance boots.

Step 2 Place the SecureNet Sensor Appliance Software CD in the CD reader and then reboot the appliance by pressing the recessed **Reset button** on the front or rear of the appliance.

A message warning you that the installation of the software from the CD will completely erase the contents of your hard disk displays. This is followed by a **boot:** prompt.

Step 3 Read the warning carefully and consider whether you want to proceed.

Step 4 If you decide that you do not want to proceed, eject the CD by pressing the **Eject button** on the front of the CD reader and then powering down the appliance
-OR-
If you decide to proceed, type:

`kvm` (if you using a keyboard and video monitor)
-OR-
`serial` (if you are using a terminal or emulator)

and then press **[Enter]**.

A prompt asks for the installation source and provides the following options: **disk**, **cdrom**, and **<URL>**.

Step 5 Type **cdrom** and then press **[Enter]**.

A prompt asks you to choose an appliance model and provides a list of choices.

Step 6 Type the model number of your appliance exactly as shown in the list and then press **[Enter]**.

Step 7 Wait for your selection to finish installing and for the Linux login prompt to display.

The CD is automatically ejected.

Step 8 Remove the CD and close the CD-ROM reader.

Step 9 At the prompt, press **[Enter]**.

The appliance reboots. Software installation from the CD is complete.

Step 10 Go to “Initially Configure Appliance” on page 2-23 and perform setup as needed.

Initially Configure Appliance

This procedure lets you initially configure the SecureNet appliance. It is required for the following appliances:

- New SecureNet Sensors with SecureNet WBI v2.x installed
- Existing SecureNet Sensors that have been upgraded by installing the SecureNet WBI v2.x software from CD

Important! If your SecureNet Sensor was upgraded using Intrusion PDS Pilot, you do not need to perform this procedure since your network parameters, software license agreement, and license key have been retained and are still valid.

To connect the external PC to the appliance, perform the following steps:

Step 1 If necessary, power on the appliance. On hardware that has a Power switch, set the **Power** switch to ON (1). On hardware without a Power switch, unplug the power cord, wait a few seconds, and then plug the power cord back into the power outlet.

Step 2 Connect an Ethernet *crossover cable* to the E1 port on the appliance and to the Ethernet port of the PC running the web browser.

Step 3 On the external PC's web browser, enter the following in the Address field:

```
sensor
```

and then press **[Enter]**. A series of new certificate dialogs display. Read and accept each dialog as requested to continue.

The SecureNet WBI Login page displays (see Figure 2-25).

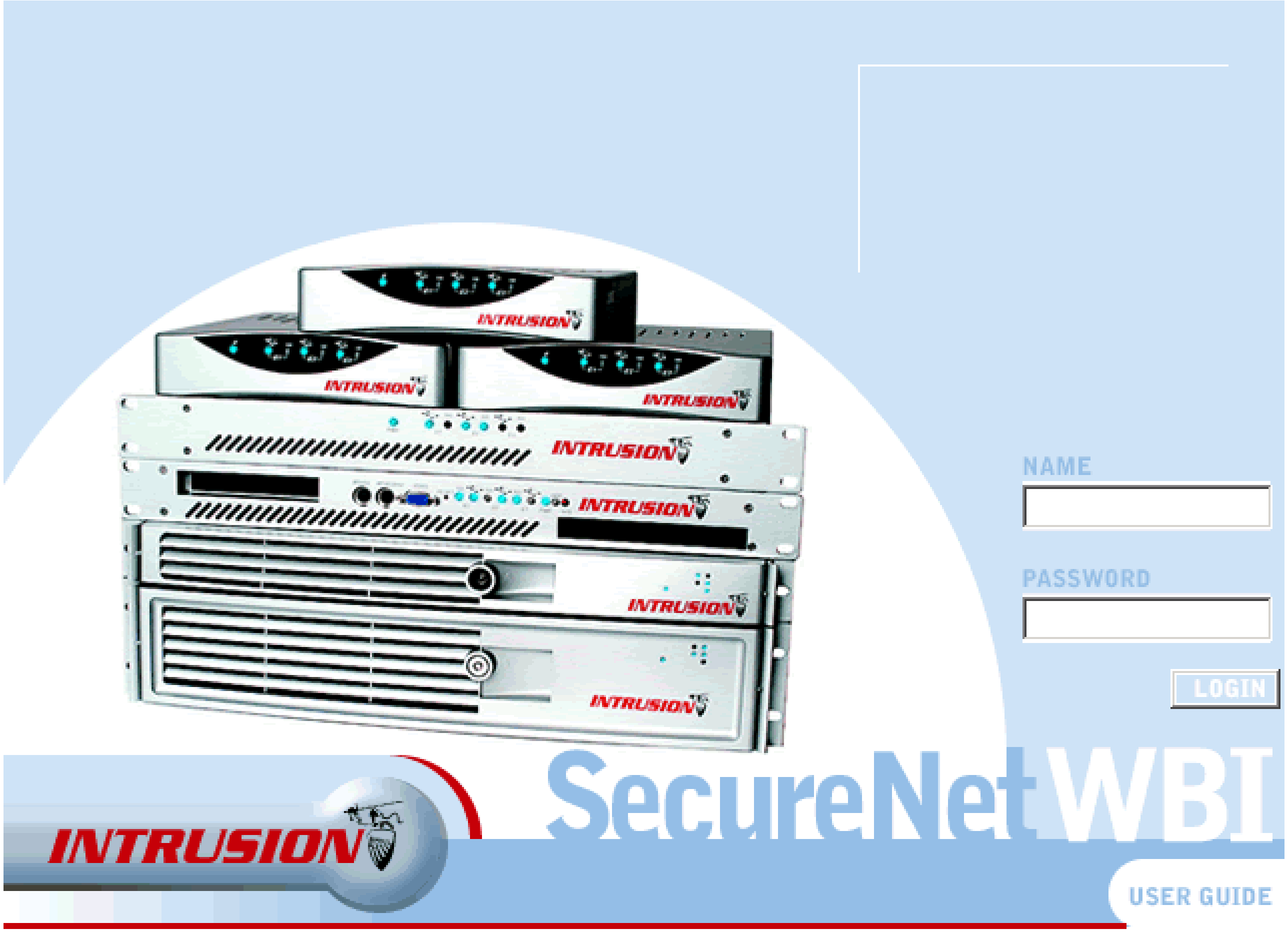
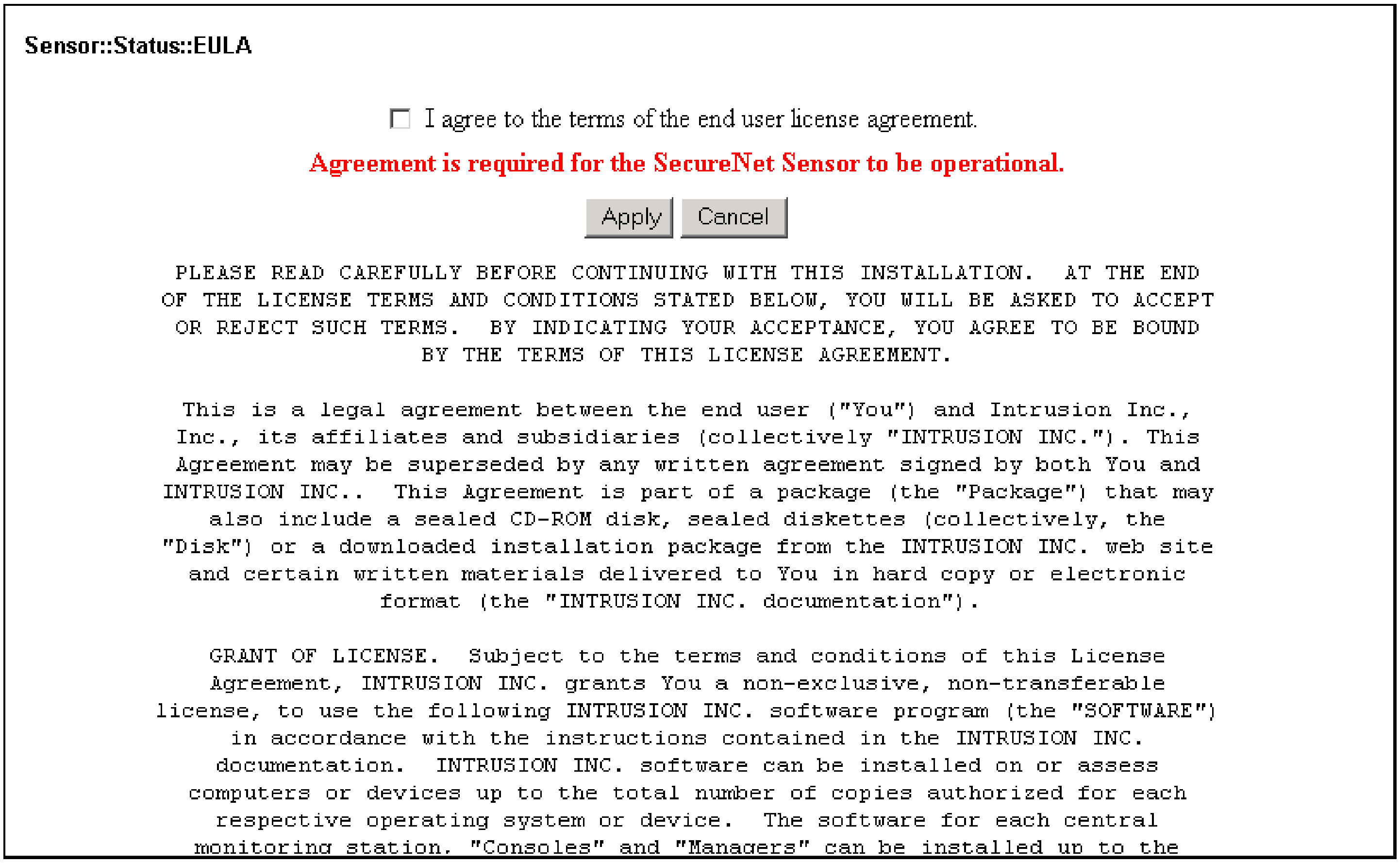


Figure 2-25 SecureNet WBI Login Page

If you are unable to connect to the SecureNet WBI Login page, check that you have correctly connected an operational crossover cable to the PC as described above.

Step 4 In the **Name** field, type “intrusion” and, in the **Password** field, type “password” and then click on the **Login** button.

The SecureNet WBI v2.x opens. If your Sensor is an existing Sensor that you have upgraded to SecureNet WBI v2.x, your acceptance of the software license agreement is already recorded and the Sensor Status page displays (see Figure 2-27). Go to page 2-26.
-OR-
If your SecureNet Sensor is new or you have upgraded the software on an existing Sensor by using the SecureNet WBI software CD, the Intrusion Software License Agreement displays (see Figure 2-26).



□ I agree to the terms of the end user license agreement.

Agreement is required for the SecureNet Sensor to be operational.

PLEASE READ CAREFULLY BEFORE CONTINUING WITH THIS INSTALLATION. AT THE END OF THE LICENSE TERMS AND CONDITIONS STATED BELOW, YOU WILL BE ASKED TO ACCEPT OR REJECT SUCH TERMS. BY INDICATING YOUR ACCEPTANCE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT.

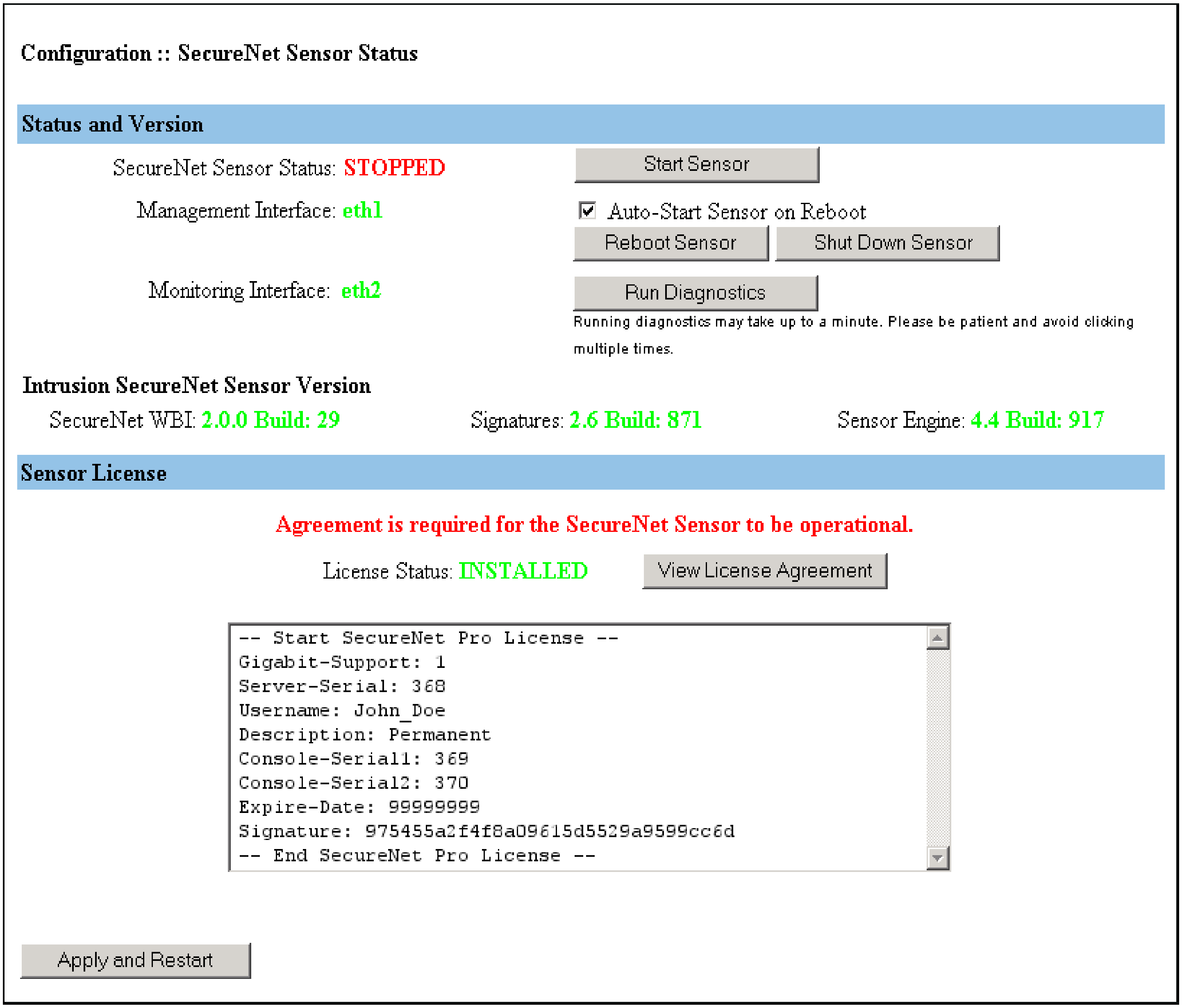
This is a legal agreement between the end user ("You") and Intrusion Inc., Inc., its affiliates and subsidiaries (collectively "INTRUSION INC."). This Agreement may be superseded by any written agreement signed by both You and INTRUSION INC.. This Agreement is part of a package (the "Package") that may also include a sealed CD-ROM disk, sealed diskettes (collectively, the "Disk") or a downloaded installation package from the INTRUSION INC. web site and certain written materials delivered to You in hard copy or electronic format (the "INTRUSION INC. documentation").

GRANT OF LICENSE. Subject to the terms and conditions of this License Agreement, INTRUSION INC. grants You a non-exclusive, non-transferable license, to use the following INTRUSION INC. software program (the "SOFTWARE") in accordance with the instructions contained in the INTRUSION INC. documentation. INTRUSION INC. software can be installed on or assess computers or devices up to the total number of copies authorized for each respective operating system or device. The software for each central monitoring station. "Consoles" and "Managers" can be installed up to the

Figure 2-26 Intrusion Software License Agreement Page

Step 5 Read the software license agreement carefully, and if you agree to the terms specified therein, click on the **Apply** button to continue.
-OR-
If you do not agree the terms of the license agreement, click on the **Cancel** button to close the page and log you out of SecureNet WBI.

When you have accepted the terms of the license agreement, the SecureNet Sensor Status page displays (see Figure 2-27).



Configuration :: SecureNet Sensor Status

Status and Version

SecureNet Sensor Status: **STOPPED**

Management Interface: **eth1**

Monitoring Interface: **eth2**

☑ Auto-Start Sensor on Reboot

Running diagnostics may take up to a minute. Please be patient and avoid clicking multiple times.

Intrusion SecureNet Sensor Version

SecureNet WBI: **2.0.0 Build: 29** Signatures: **2.6 Build: 871** Sensor Engine: **4.4 Build: 917**

Sensor License

Agreement is required for the SecureNet Sensor to be operational.

License Status: **INSTALLED**

```
-- Start SecureNet Pro License --
Gigabit-Support: 1
Server-Serial: 368
Username: John_Doe
Description: Permanent
Console-Serial1: 369
Console-Serial2: 370
Expire-Date: 99999999
Signature: 975455a2f4f8a09615d5529a9599cc6d
-- End SecureNet Pro License --
```

Figure 2-27 SecureNet Sensor Status Page

The SecureNet Sensor Status page displays the current status of the appliance. When you first log in to the Sensor, its Status is STOPPED, its License Status displays INSTALLED if you are upgrading an existing Sensor or NOT INSTALLED if you are installing a new Sensor (or if you are installing a Sensor that has been upgraded by using the SecureNet Sensor with SecureNet WBI v2.x Software CD).

Note If the License Status displays NOT INSTALLED, you must install a valid license key before attempting to configure or run the SecureNet Sensor. The license key is obtained by sending an e-mail to the Intrusion License Administrator at help@intrusion.com. After the License Administrator has validated your purchase, the license key will be sent to you via e-mail.

Step 6 If the License Status displays NOT INSTALLED, enter the license key in the **License Key** text box exactly as received from the Intrusion License Administrator. To ensure accuracy, copy the license key from the e-mail and paste it into the **License Key** text box.

Step 7 When you have completed entering the license key, click on the **Apply and Restart** button.

The SecureNet Sensor restarts (if it is already running).

Step 8 Log back in to the SecureNet WBI and verify that the License Status displays INSTALLED.

If the License Status displays NOT INSTALLED, compare the text in the License Key text box with the text received from the Intrusion License Administrator, go back to Step 6 and correct as needed.

Step 9 Start the Sensor, if necessary, by clicking on the **Start Sensor** button.

The Sensor Status displays RUNNING.

Step 10 If your appliance has not been configured for your network or you want to change the configuration settings for the Sensor, go to "Configure Networking" on page 3-20 and perform the appropriate procedures.

Important! Be sure to go to "Configure User Access Options" on page 3-37 and change your password from the default "password".

Installation is complete.

Logging In to SecureNet WBI

To log in to the SecureNet WBI, perform the following steps:

Step 1 On a Microsoft Internet Explorer (version 5 or greater) web browser's address field, type the URL assigned to the Ethernet port *eth1* on your Sensor (https://<*ipaddress*>) and then press **[Enter]**.

The SecureNet WBI Login page displays (see Figure 2-25).

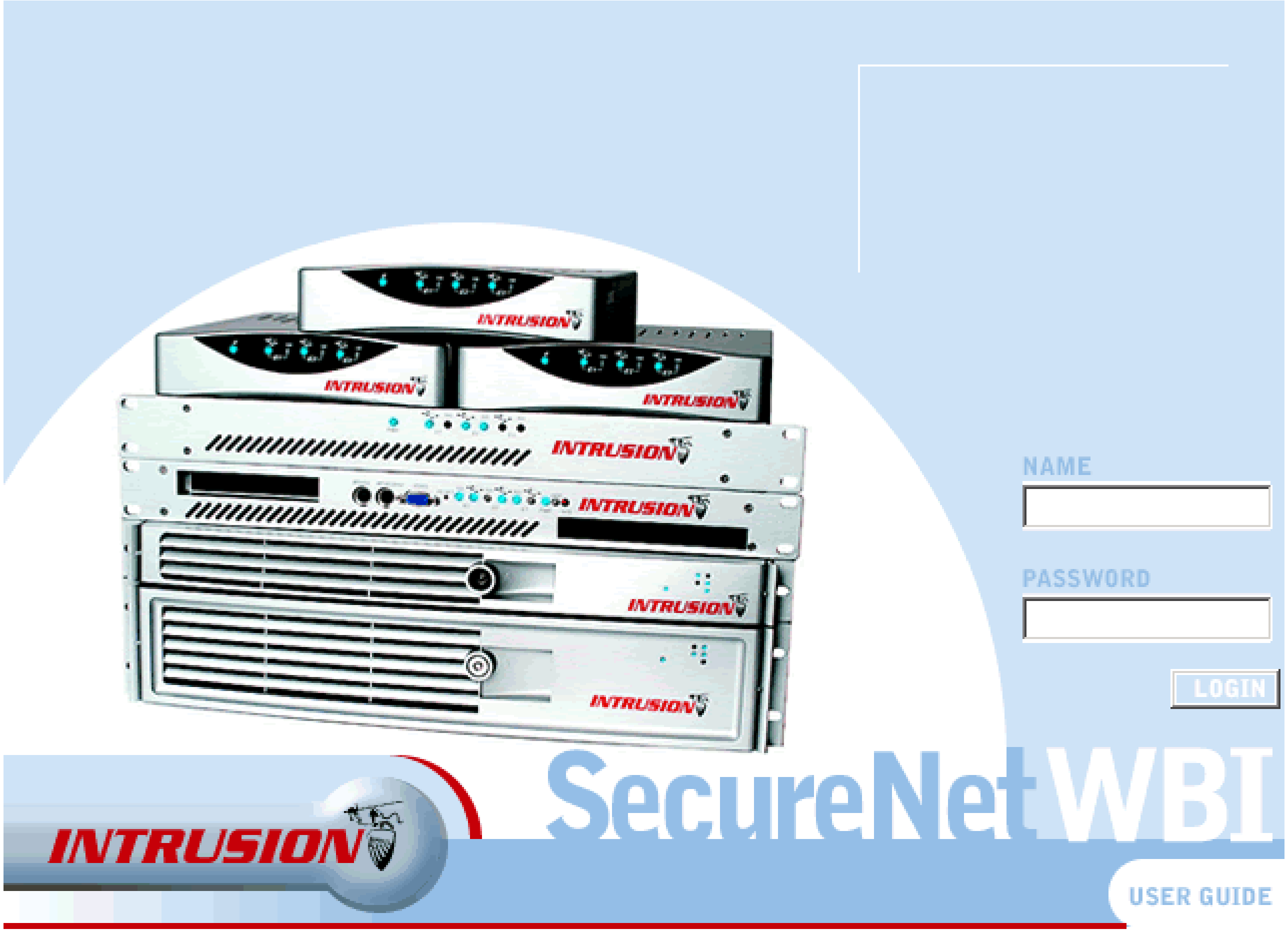


Figure 2-28 SecureNet WBI Login Page

This page lets you log in to the Intrusion SecureNet WBI. You can also access the user guide (as a PDF document) by clicking on the **User Guide** link in the lower right corner.

Step 2 Type your administrator username and password in the fields provided.

The Password field displays all characters as asterisks to prevent inadvertent disclosure.

Step 3 Click on the **Login** button.

When you have logged in successfully, the Intrusion SecureNet WBI opens. The page that displays by default is the SecureNet Sensor Status page (see Figure 2-27). If you want a different page to display upon opening SecureNet WBI, refer to Chapter 3 in this user guide where you can specify the page that you want displayed upon opening SecureNet WBI.

Most SecureNet WBI pages display a header at the top of the page (see Figure 2-29).

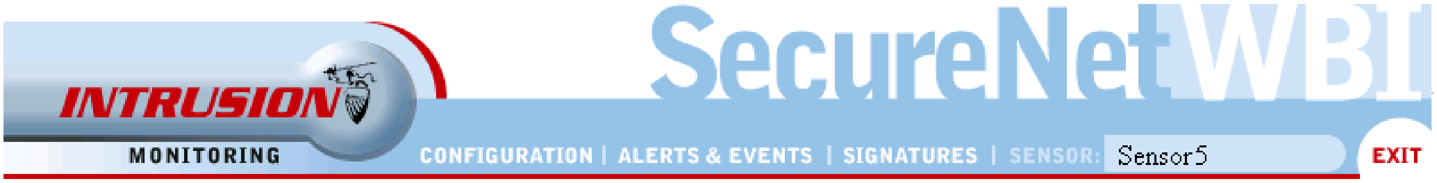
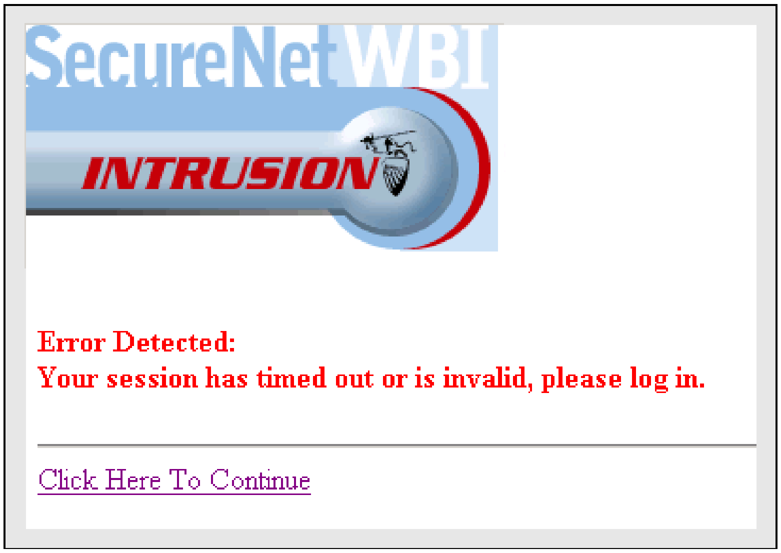


Figure 2-29 Intrusion SecureNet WBI Page Header

The header displays the current name of the Sensor and provides a Navigation bar with buttons that display drop-down menus of options from which you can select an activity that you want to perform:

- **Monitoring**—lets you monitor the events detected by your SecureNet Sensor. Refer to "Monitoring Options" on page 4-1.
- **Configuration**—lets you make changes to the way that the SecureNet Sensor operates. Refer to "Configuration Menu Options" on page 3-2.
- **Alerts & Events**—lets you configure SecureNet WBI monitoring, SecureNet Provider, email alerting and SNMP alerting for your appliance. Refer to "Configure Alerts & Events Options" on page 3-42.
- **Signatures**— lets you customize the attack signatures for the SecureNet Sensor. Refer to "Configure Signatures Menu Options" on page 3-47.
- **Exit**—lets you log out of SecureNet WBI. Refer to "Exit Options" on page 2-31.

Reminder If you are on any page of the SecureNet WBI other than the Monitoring page and you leave the interface idle for the period specified as the timeout (the default is 10 minutes), you will automatically be logged out of SecureNet WBI. After the timeout, when you try to perform any action, you will receive the error message shown below.



Error Detected:
Your session has timed out or is invalid, please log in.

Click on the **Click Here To Continue** link to go to the SecureNet WBI Login page.

Exit Options

The Exit menu (see Figure 2-30) lets you log out of the Intrusion SecureNet WBI.

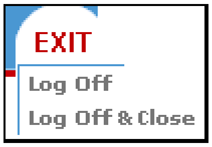
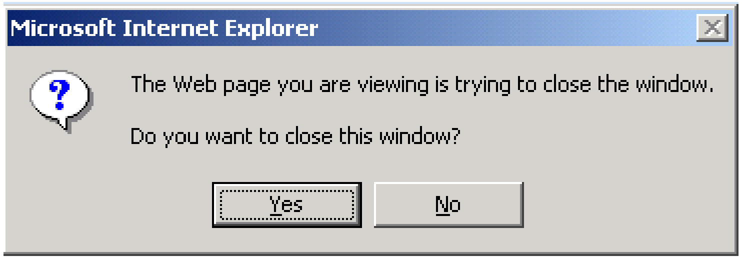


Figure 2-30 Exit Menu

To log out of Intrusion SecureNet WBI, perform the following steps:

Step 1 From any Intrusion SecureNet WBI page, choose **Exit>Log Off** or **Exit>Log Off & Close**.

If you choose Exit>Log Off, SecureNet WBI closes and the SecureNet WBI Login page is displayed; if you choose Exit>Log Off & Close, SecureNet WBI closes and the Close Window dialog displays (see Figure 2-31).



The Web page you are viewing is trying to close the window.

Do you want to close this window?

Figure 2-31 Close Window Dialog

Step 2 To close the window, click on the **Yes** button.
-OR-
If you have changed your mind and want to leave the window open, click on the **No** button and the SecureNet WBI Login page displays.

Chapter 3

Configuring the SecureNet Sensor

This chapter provides the procedures for using the Intrusion SecureNet WBI to configure your SecureNet Sensor and the SecureNet WBI for use. It includes instructions for using all the options that are in the Configuration, Alerts & Events, and Signatures menus.

The procedures in this chapter can be randomly accessed. If you are reading this guide using a PDF reader, you can use the Table of Contents, use the search capabilities of the PDF reader, or use the PDF bookmarks in the reader's Navigation pane to find topics of interest. If you are reading this guide on hardcopy, you can use the Table of Contents and the reference lists provided in this chapter to help you locate the procedure you want to perform.

- For CONFIGURATION menu options, go to "Configuration Menu Options" on page 3-2.
- For ALERTS & EVENTS menu options, go to "Configure Alerts & Events Options" on page 3-42.
- For SIGNATURES menu options, go to "Configure Signatures Menu Options" on page 3-47.

Configuration Menu Options

The Configuration menu (see Figure 3-1) can be accessed from any Intrusion SecureNet WBI page.

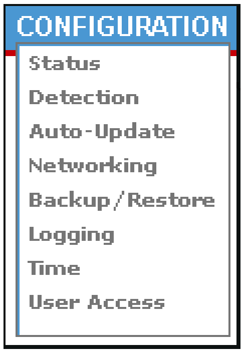


Figure 3-1 Configuration Menu

Note Depending on your software license, some options may be disabled on the Configuration menu.

From the Configuration menu, you can view and edit configuration options as described in the following sections:

"Configure Sensor Status" on page 3-5

- "Start/Stop SecureNet Sensor Daemon" on page 3-5
- "Reboot Sensor" on page 3-6
- "Shut Down Sensor" on page 3-6
- "Change SecureNet Sensor Reboot Status" on page 3-6
- "View/Edit License Key" on page 3-8
- "View Software License Agreement" on page 3-9

"Configure Detection Options" on page 3-11

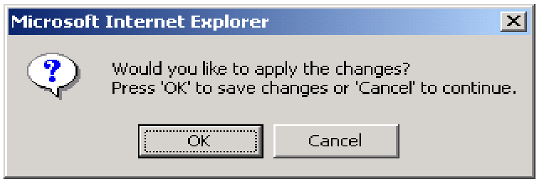
- "Configure Global Filtering" on page 3-11
- "Configure Source/Destination MAC Address Filters" on page 3-13
- "Configure Source/Destination IP Address Filters" on page 3-13
- "Configure Source/Destination Port Filters" on page 3-13
- "Configure VLAN Filtering" on page 3-14
- "Configure State Settings" on page 3-15
- "Configure Sensor Settings" on page 3-16
- "Configure Advanced Detection" on page 3-16
- "Configure Monitored Hosts" on page 3-16
- "Configure Monitored Ranges" on page 3-17

"Configure Auto-Update" on page 3-18

Important! The default view of the Configuration pages is **Basic**. Some Configuration pages contain links labeled **Advanced** which, when clicked, display detailed views. On these pages, there is also a checkbox (generally at the bottom of the page adjacent to an **Apply and Restart** button) that you can select so that the Advanced view is always shown.

The Advanced view of the Configuration page lets you configure various settings for the Sensor. You should, however, exercise extreme care not to make changes that you do not thoroughly understand. Poorly planned configuration changes can have a dramatic adverse affect on a Sensor’s performance. The default settings for the Sensor should be sufficient for typical use. If you need help, contact Intrusion Technical Support for advice.

Note If you make changes to the configuration in any area of the Configuration page, you must scroll to the bottom of the page to click on the **Apply and Restart** button to apply your changes and restart the Sensor, or you must save your changes when the following dialog displays:



Would you like to apply the changes?
Press 'OK' to save changes or 'Cancel' to continue.

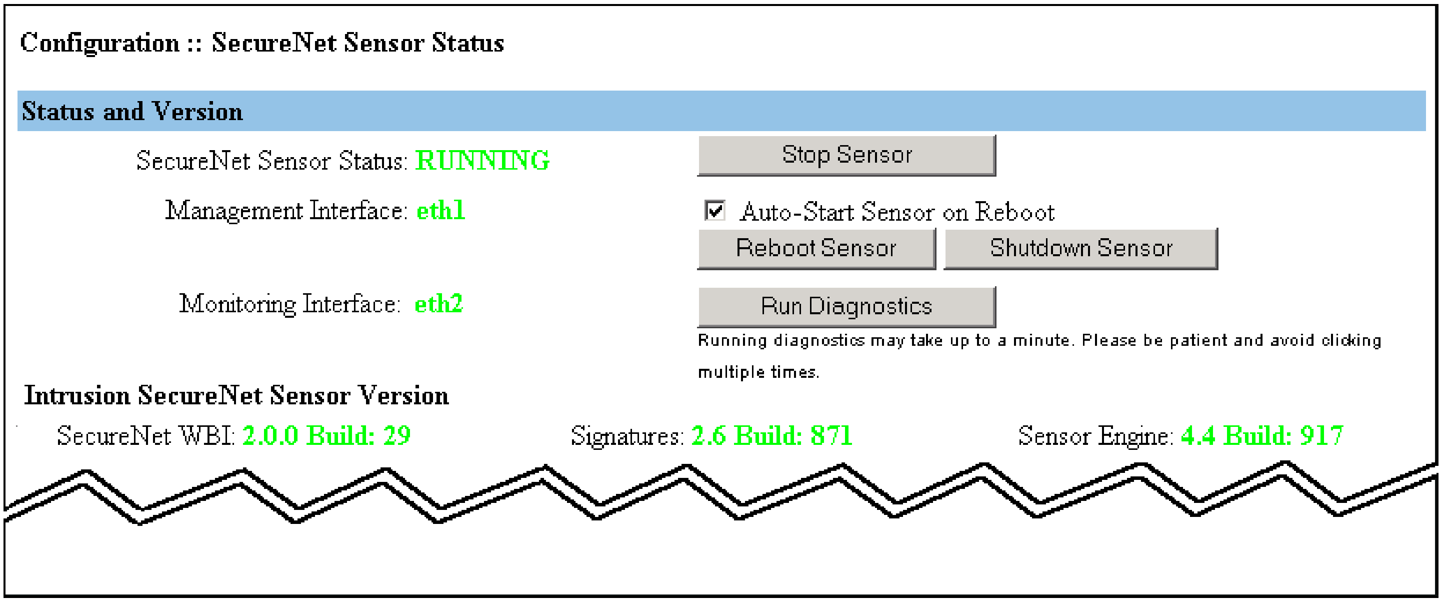
Because many of the Configuration pages are long, we have used a divider in some illustrations to indicate that the page shown is not complete and that you may need to scroll down to see the portion of the page shown:

Configure Sensor Status

To view the current status of the SecureNet Sensor, perform the following steps:

Step 1 At the top of any Intrusion SecureNet WBI page, click on the **Configuration** menu and then choose **Status**.

The SecureNet Sensor Status Configuration page displays (see Figure 3-2).



Configuration :: SecureNet Sensor Status

Status and Version

SecureNet Sensor Status: RUNNING

Management Interface: eth1

Monitoring Interface: eth2

☑ Auto-Start Sensor on Reboot

Running diagnostics may take up to a minute. Please be patient and avoid clicking multiple times.

Intrusion SecureNet Sensor Version

SecureNet WBI: 2.0.0 Build: 29

Signatures: 2.6 Build: 871

Sensor Engine: 4.4 Build: 917

Figure 3-2 SecureNet Sensor Status Configuration Page (Status and Version)

The Status and Version area of the SecureNet Sensor Status Configuration page lets you view the status of the SecureNet Sensor at a glance:

- **SecureNet Sensor Status**—displays whether the SecureNet Sensor daemon is currently stopped or running.
- **Management Interface**—identifies the appliance's ethernet port that is being used to access SecureNet WBI to manage the appliance.
- **Monitoring Interface**—identifies the ethernet port that the Sensor is using to monitor your network.
- **SecureNet WBI version**—displays the version and build number of the Intrusion SecureNet WBI that you are currently using.
- **Signatures version**—displays the version and build number of the attack signature pack currently being used.
- **Sensor Engine version**—displays the version and build number of the SecureNet Sensor engine software currently running.

Start/Stop SecureNet Sensor Daemon

To start or stop the SecureNet Sensor, perform the following steps:

Step 1 On the Status area at the top of the SecureNet Sensor Status Configuration page (see Figure 3-2), click on the **Start Sensor/Stop Sensor** button.

Step 2 Wait until the SecureNet Sensor Status changes to reflect your selection (shows RUNNING or STOPPED).

Important! Be patient. Do not repeatedly click on the **Start Sensor/Stop Sensor** button. It may take a minute or more for the SecureNet Sensor Status to change.

Change SecureNet Sensor Reboot Status

When the **Auto-Start on Reboot** button in the Status area is checked, the SecureNet Sensor is automatically started when the Sensor is rebooted. To change the reboot status, perform the following steps:

Step 1 On the Status area at the top of the SecureNet Sensor Status Configuration page (see Figure 3-2), click on the **Auto-Start on Reboot** button.

The status changes. If the checkbox was checked, it is now unchecked. If it was unchecked, it is now checked.

Step 2 Scroll down to the bottom of the page and click on the **Apply and Restart** button to apply your changes and restart the Sensor.

Reboot Sensor

Step 1 On the Status area at the top of the SecureNet Sensor Status Configuration page (see Figure 3-2), click on the **Reboot Sensor** button.

The SecureNet WBI login page displays (see "SecureNet WBI Login Page" on page 2-15).

Step 2 Wait a few minutes to allow the Sensor to complete the reboot process and then log in to the SecureNet Sensor using your user name and password.

If the browser displays a **This Page cannot be displayed** message, the Sensor has not completed the reboot process. Wait a short while longer and repeat this step.

Shut Down Sensor

To shut down the Sensor appliance, perform the following steps:

Step 1 On the Status area at the top of the SecureNet Sensor Status Configuration page (see Figure 3-2), click on the **Shut Down Sensor** button.

A confirmation dialog displays.

Step 2 Click on the **OK** button.

The SecureNet Sensor appliance shuts down. You can power off the appliance.

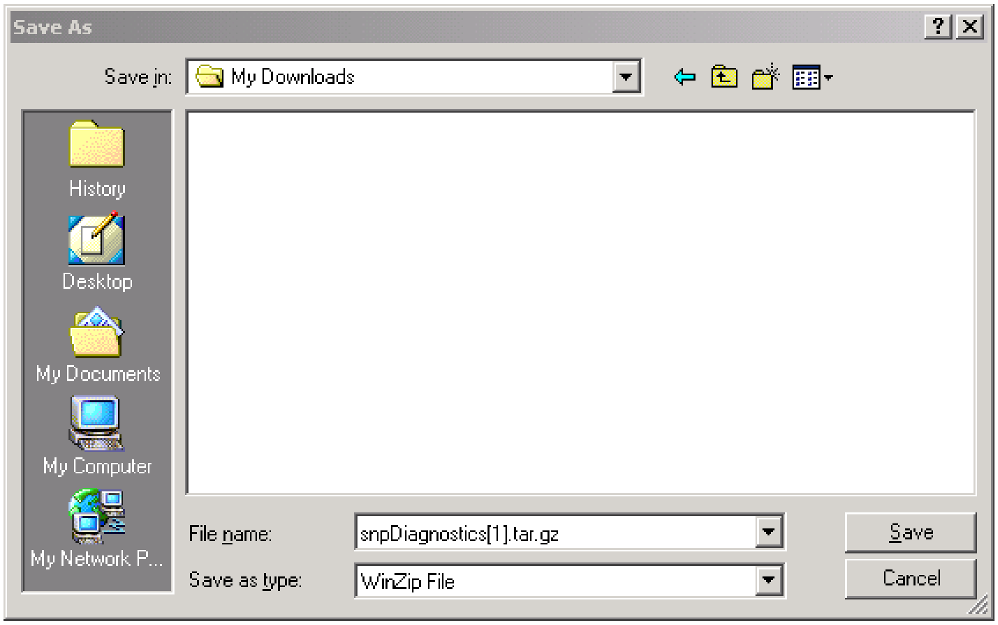
Run Sensor Diagnostics

The Sensor Diagnostics function provides you with a compressed file that contains other information files that you can send to Intrusion Technical Support when they are helping you troubleshoot the Sensor. Generally, you will be asked to email the compressed file to Intrusion.

To run diagnostics on the SecureNet Sensor appliance, perform the following steps:

Step 1 On the Status area at the top of the SecureNet Sensor Status Configuration page (see Figure 3-2), click on the **Run Diagnostics** button.

A Save As dialog displays (see Figure 3-3).



Save in: My Downloads

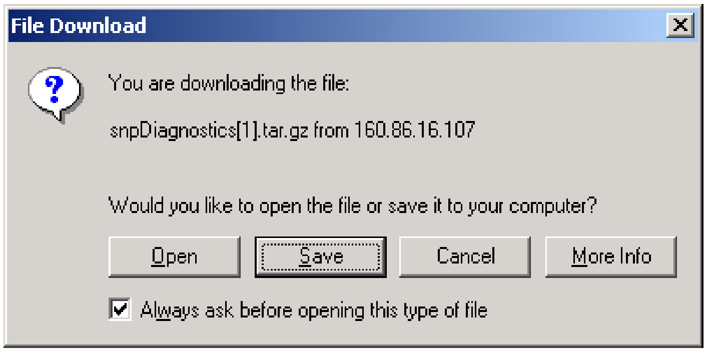
File name: snpDiagnostics[1].tar.gz

Save as type: WinZip File

Figure 3-3 Save As Dialog

Step 2 Use the **Save In** pull-down list as needed to locate the folder on your workstation into which you want to save the diagnostic compressed file (a TGZ file that can be opened using WinZip) and then click on the **Save** button.

A File Download dialog displays (see Figure 3-4).



You are downloading the file:

snpDiagnostics[1].tar.gz from 160.86.16.107

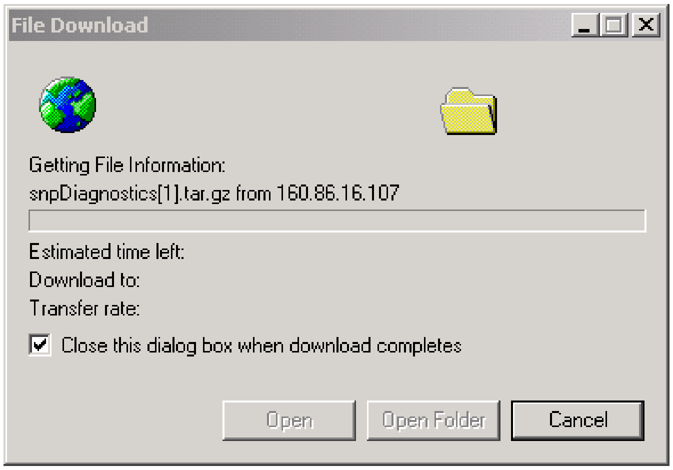
Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

Figure 3-4 File Download Dialog

Step 3 Click on the **Save** button to save the file to the designated folder on your workstation's hard disk.

A File Download progress dialog displays (see Figure 3-5).



Getting File Information:
snpDiagnostics[1].tar.gz from 160.86.16.107

Estimated time left:
Download to:
Transfer rate:

☑ Close this dialog box when download completes

Figure 3-5 File Download Progress Dialog

Step 4 Click on the **Close this dialog box when download completes** checkbox to select it. Wait for the download process to complete.

The dialog closes.

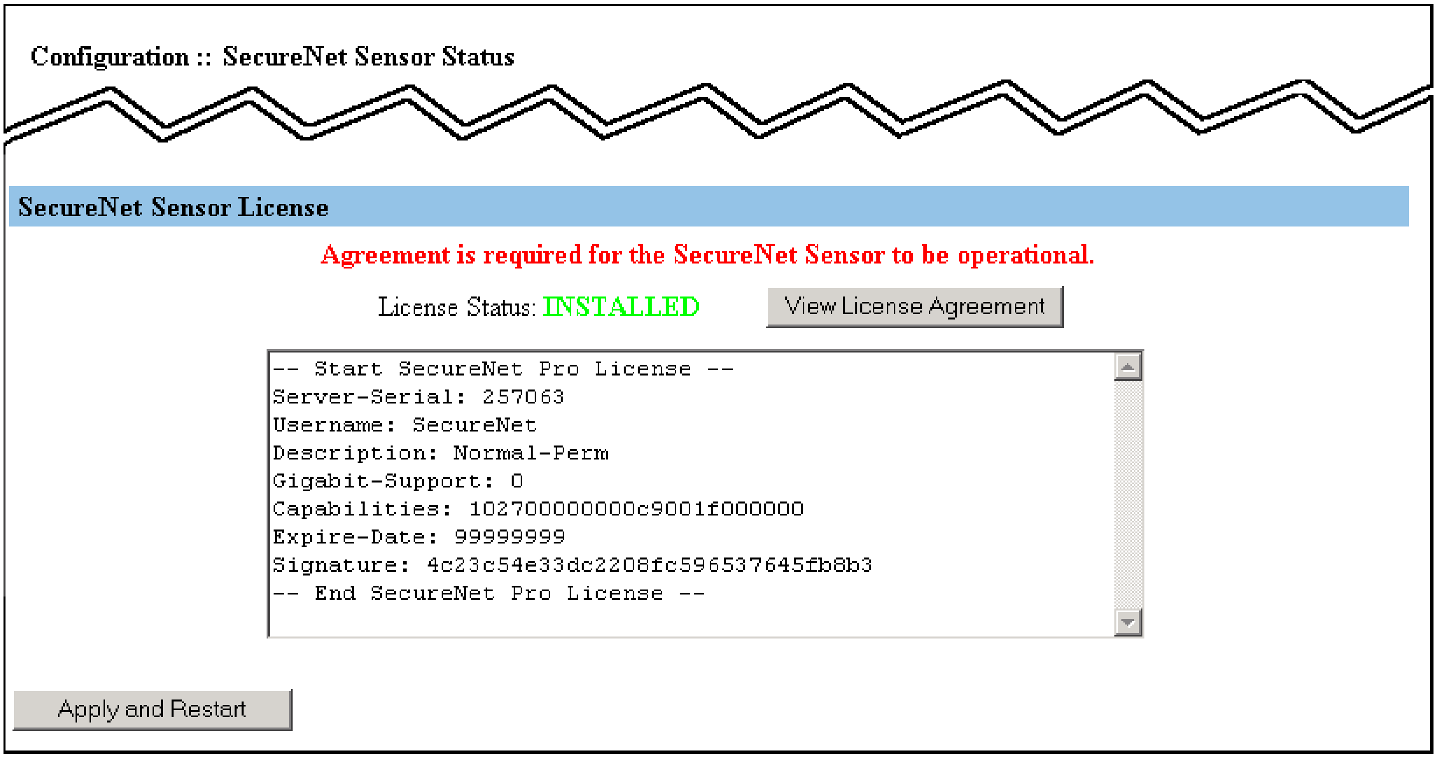
Step 5 Locate the downloaded file and, upon their request, email it as an attachment to Intrusion Technical Support.

View/Edit License Key

To view/edit the SecureNet Sensor license key for the Sensor, perform the following steps:

Step 1 If necessary, scroll down to the Sensor License area of the SecureNet Sensor Status Configuration page.

The Sensor License area of the Status Configuration page displays (see Figure 3-6).



Configuration :: SecureNet Sensor Status

SecureNet Sensor License

Agreement is required for the SecureNet Sensor to be operational.

License Status: INSTALLED

```
-- Start SecureNet Pro License --
Server-Serial: 257063
Username: SecureNet
Description: Normal-Perm
Gigabit-Support: 0
Capabilities: 102700000000c9001f000000
Expire-Date: 99999999
Signature: 4c23c54e33dc2208fc596537645fb8b3
-- End SecureNet Pro License --
```

Figure 3-6 SecureNet Sensor Status Configuration Page (Sensor License)

This area of the Status Configuration page displays whether the SecureNet license key has been found. It also lets you type or edit the Sensor license key sent to you by the Intrusion License Administrator in an e-mail.

Step 2 In the text box, type (or use copy-and-paste) the SecureNet Sensor license key *exactly* as provided to you.

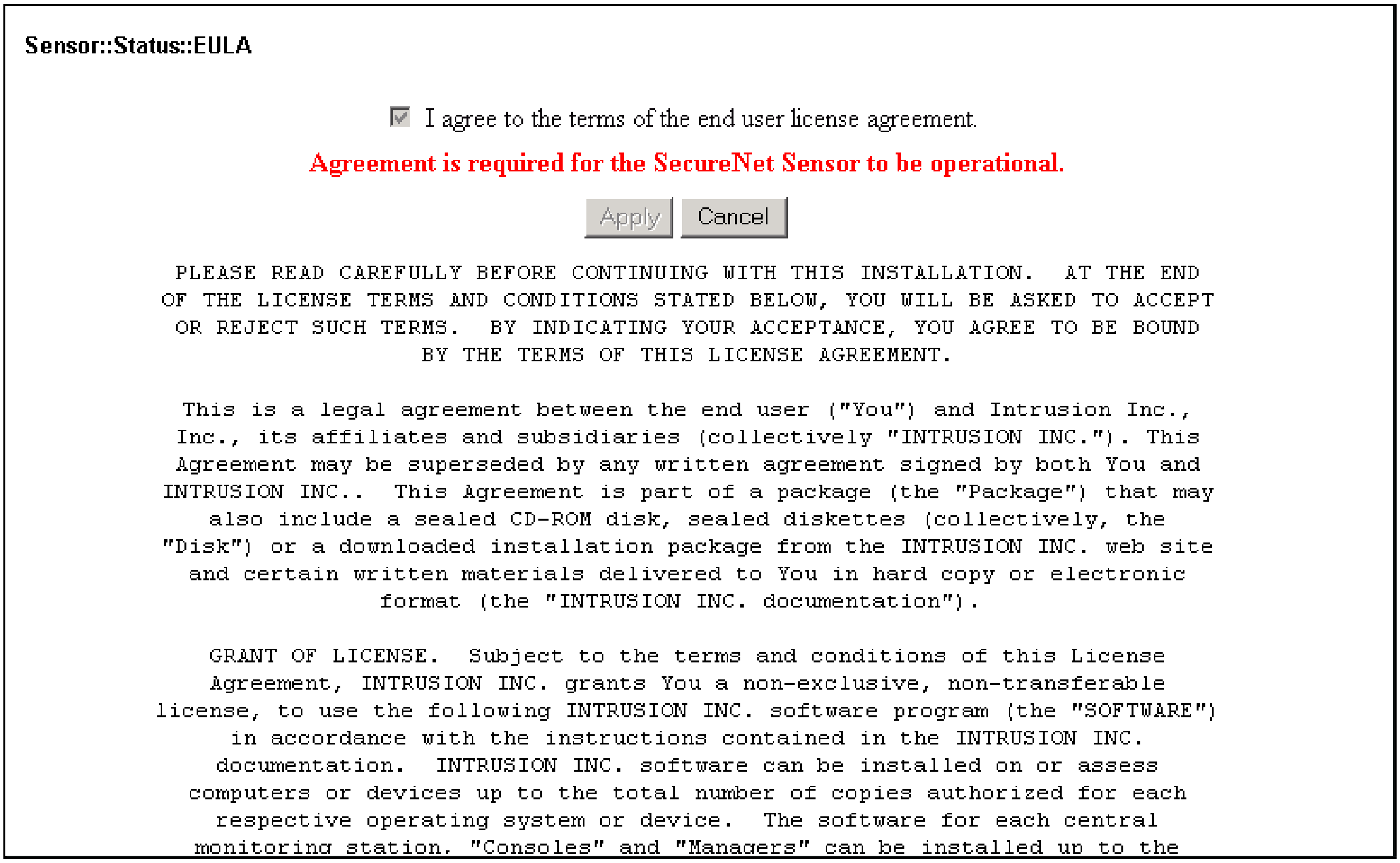
Step 3 When you are finished changing the text for the license key, save your changes by clicking on the **Apply and Restart** button.

View Software License Agreement

To view the Intrusion software license agreement, perform the following steps:

Step 1 On the lower portion of the SecureNet Sensor Status Configuration page (see Figure 3-6), click on the **View License Agreement** button.

The License Agreement page displays in a new browser window (see Figure 3-6).



Sensor::Status::EULA

☑ I agree to the terms of the end user license agreement.

Agreement is required for the SecureNet Sensor to be operational.

```
PLEASE READ CAREFULLY BEFORE CONTINUING WITH THIS INSTALLATION.  AT THE END
OF THE LICENSE TERMS AND CONDITIONS STATED BELOW, YOU WILL BE ASKED TO ACCEPT
OR REJECT SUCH TERMS.  BY INDICATING YOUR ACCEPTANCE, YOU AGREE TO BE BOUND
BY THE TERMS OF THIS LICENSE AGREEMENT.

This is a legal agreement between the end user ("You") and Intrusion Inc.,
Inc., its affiliates and subsidiaries (collectively "INTRUSION INC."). This
Agreement may be superseded by any written agreement signed by both You and
INTRUSION INC..  This Agreement is part of a package (the "Package") that may
also include a sealed CD-ROM disk, sealed diskettes (collectively, the
"Disk") or a downloaded installation package from the INTRUSION INC. web site
and certain written materials delivered to You in hard copy or electronic
format (the "INTRUSION INC. documentation").

GRANT OF LICENSE.  Subject to the terms and conditions of this License
Agreement, INTRUSION INC. grants You a non-exclusive, non-transferable
license, to use the following INTRUSION INC. software program (the "SOFTWARE")
in accordance with the instructions contained in the INTRUSION INC.
documentation.  INTRUSION INC. software can be installed on or assess
computers or devices up to the total number of copies authorized for each
respective operating system or device.  The software for each central
monitoring station. "Consoles" and "Managers" can be installed up to the
```

Figure 3-7 Intrusion Software License Agreement Page

Since you have previously agreed to the terms of the software license agreement, the checkbox for accepting the agreement is grayed.

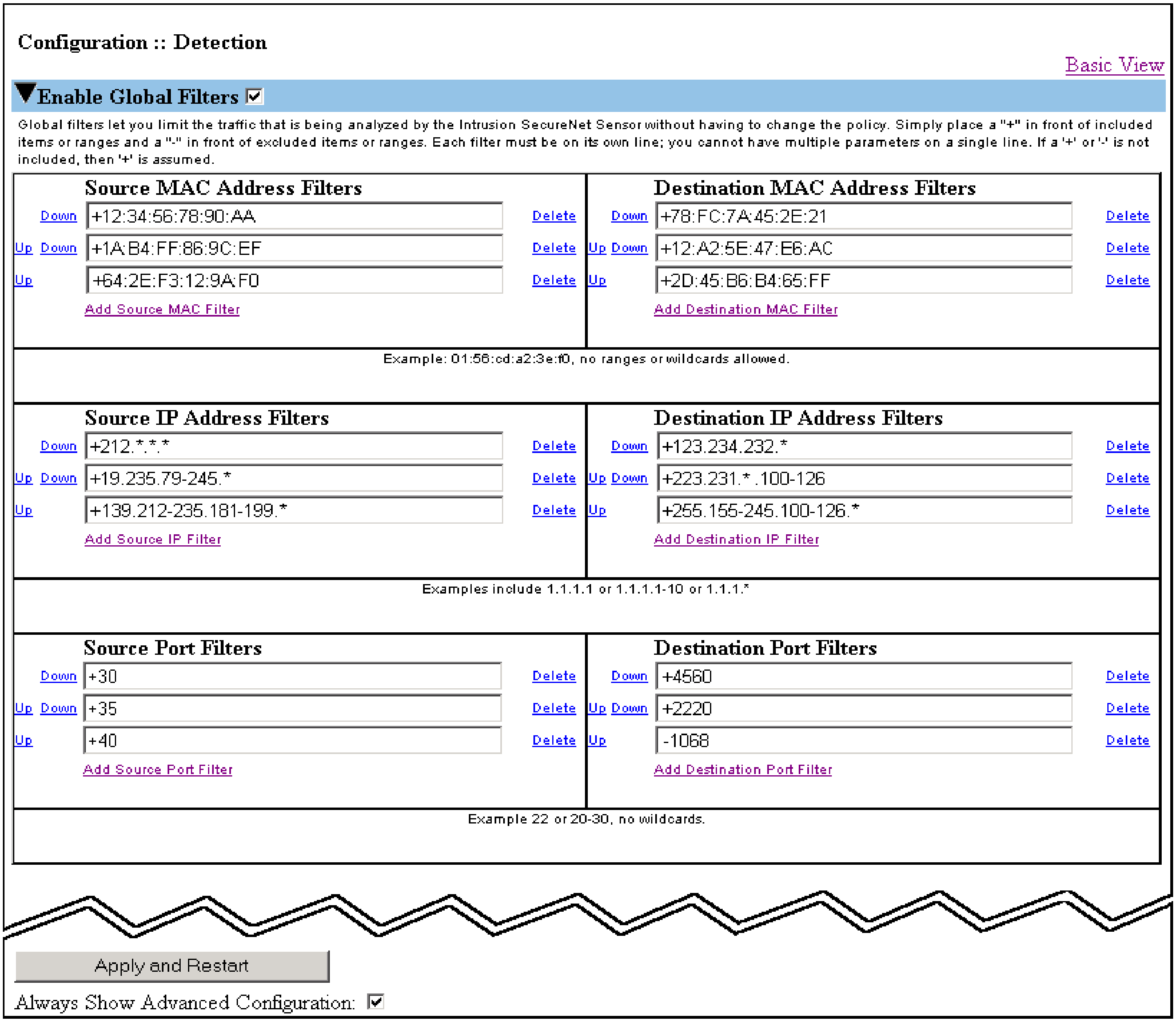
Step 2 To close the window, click on the **X** in the upper right corner.

Configure Detection Options

Configure Global Filtering

Step 1 At the top of any Intrusion SecureNet WBI page, click on the **Configuration** menu and then choose **Detection**.

The Detection Configuration page displays the Enable Global Filters area as shown in Figure 3-8.



Configuration :: Detection

▼Enable Global Filters ☑

Global filters let you limit the traffic that is being analyzed by the Intrusion SecureNet Sensor without having to change the policy. Simply place a "+" in front of included items or ranges and a "-" in front of excluded items or ranges. Each filter must be on its own line; you cannot have multiple parameters on a single line. If a '+' or '-' is not included, then '+' is assumed.

Source MAC Address Filters

- +12:34:56:78:90:AA
- +1A:B4:FF:86:9C:EF
- +64:2E:F3:12:9A:F0

Destination MAC Address Filters

- +78:FC:7A:45:2E:21
- +12:A2:5E:47:E6:AC
- +2D:45:B6:B4:65:FF

Example: 01:56:cd:a2:3e:f0, no ranges or wildcards allowed.

Source IP Address Filters

- +212.*.*.*
- +19.235.79-245.*
- +139.212-235.181-199.*

Destination IP Address Filters

- +123.234.232.*
- +223.231.*.100-126
- +255.155-245.100-126.*

Examples include 1.1.1.1 or 1.1.1.1-10 or 1.1.1.*

Source Port Filters

- +30
- +35
- +40

Destination Port Filters

- +4560
- +2220
- -1068

Example 22 or 20-30, no wildcards.

Always Show Advanced Configuration: ☑

Figure 3-8 Detection Configuration Page (Global Filtering)

The upper portion of the page lets you enable Global Filtering and specify the rules for event filtering that you want done. The Global Filtering portion is arranged with source addresses and ports on the left and destination addresses and ports on the right.

In all cases where you enter a port number or address in a global filtering rule, that rule is checked to make sure it is valid and complete. Error messages are generated for invalid rule entries.

Note Global filtering rules provide a means of specifying what traffic is looked at by the Sensor. Combinations of the following formatting characters can be specified in source and destination fields to enable flexible event monitoring through the inclusion, exclusion, and listing of multiple IP addresses, MAC addresses, or port numbers:

***** A wildcard character (*) specifies that any valid number should be included for a part of an IP address, a MAC address, or a port number. For example, specifying 1.1.1.* on an IP address line would include all valid numbers for the last quad in the address, and this would include all Class C IP addresses.

- A dash (-) indicates a range of IP addresses, MAC addresses, or port numbers. For example, you can use a dash to specify the range for an IP address class: 1.1.1.0-222.

+ To *include* an IP address, a MAC address, or a port number for monitoring, type a plus sign (+) before the address or port number. If no character precedes a source or destination, *inclusion* is the default.

- To *exclude* an IP address, a MAC address, or a port number from monitoring, type a dash or minus sign (-) before the address or port number.

For more information about event filtering and the specification of fields, refer to Appendix A, “Field Formatting and Event Filtering”.

Important! Filter rules *must* be listed in the order of precedence. Rules at the top of a list are considered first, and rules at the end of a list are considered last. For example, to monitor all packets to the subnet 10.20.20.x, except for IP address 10.20.20.55, the following rules should be entered:

-10.20.20.55
+10.20.20.*

In this example, due to the order of precedence, the IP address of a given packet is first compared to 10.20.20.55 to determine if it should be discarded, before comparing it to 10.20.20.* to determine if it should be analyzed by the Sensor.

Each filter rules list has **Up** and **Down** links that let you move rules in that list up or down, respectively, as needed to place the rules in the proper order.

Configure Source/Destination MAC Address Filters

Step 2 To add a source/destination MAC address rule to the global filter:

a. Click on the **Add Source MAC Filter** or the **Add Destination MAC Filter** link.

A blank text field displays.

b. Type a MAC address using the format *xx:xx:xx:xx:xx:xx*, where *xx* is any hexadecimal value *00-FF*. The field is not case-sensitive. The wildcard (*) and range (-) characters can be used.

Step 3 To move a source/destination MAC address rule up or down in the list, click on its **Up** or **Down** link as needed to position the address appropriately in the list.

Step 4 To delete a source/destination MAC address from the list, click on the **Delete** link to the right of the address in the list.

Step 5 When you have finished configuring the source/destination MAC address rules for the global filter, scroll down to the bottom of the page and click on the **Apply and Restart** button.

The Sensor restarts and begins using your new global filtering rules.

Configure Source/Destination IP Address Filters

Step 6 To add a source/destination IP address rule to the global filter:

a. Click on the **Add Source IP Filter** or the **Add Destination IP Filter** link.

A blank text field displays.

b. Type an IP address using dotted quad format *x.x.x.x*, where *x* is a decimal value 0-255. The wildcard (*) and range (-) characters can be used.

Step 7 To move a source/destination IP address rule up or down in the list, click on its **Up** or **Down** link as needed to position the address appropriately in the list.

Step 8 To delete a source/destination IP address from the list, click on the **Delete** link to the right of the address in the list.

Step 9 When you have finished configuring the source/destination IP address rules for the global filter, scroll down to the bottom of the page and click on the **Apply and Restart** button.

The Sensor reboots and starts using your new global filtering rules.

Configure Source/Destination Port Filters

Step 10 To add a source/destination Port number rule to the global filter:

a. Click on the **Add Source Port Filter** or the **Add Destination Port Filter** link.

A blank text field displays.

b. Type a UDP or TCP port number of format *x*, where *x* is a value between 0 and 65535. The wildcard (*) and range (-) characters can be used.

Step 11 To move a source/destination Port number rule up or down in the list, click on its **Up** or **Down** link as needed to position the address appropriately in the list.

Step 12 To delete a source/destination Port number rule from the list, click on the **Delete** link to the right of the Port number in the list.

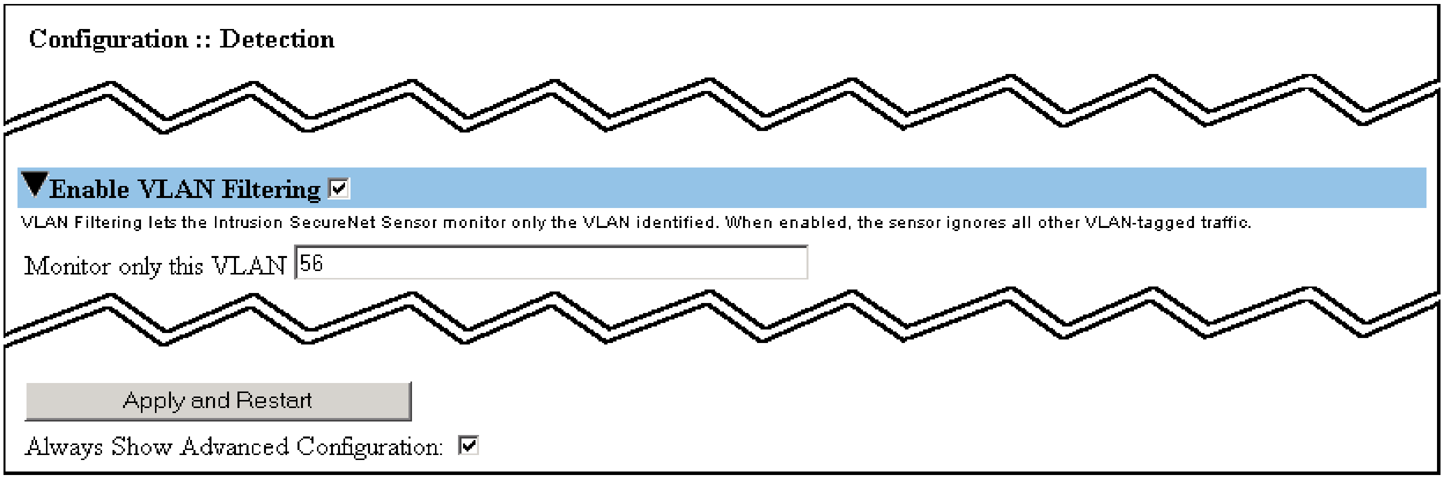
Step 13 When you have finished configuring the source/destination Port number rules for the global filter, scroll down to the bottom of the page and click on the **Apply and Restart** button.

The Sensor restarts and begins using your new global filtering rules.

Configure VLAN Filtering

To configure VLAN Filtering for the SecureNet Sensor, perform the following steps:

Step 14 Scroll down the Detection Configuration page to display the VLAN Filtering area of the page (see Figure 3-9).



Configuration :: Detection

▼Enable VLAN Filtering ☑

VLAN Filtering lets the Intrusion SecureNet Sensor monitor only the VLAN identified. When enabled, the sensor ignores all other VLAN-tagged traffic.

Monitor only this VLAN 56

Always Show Advanced Configuration: ☑

Figure 3-9 Detection Configuration Page (Enable VLAN Filtering)

This portion of the Configure Detection page lets you enable/disable VLAN filtering. When VLAN filtering is enabled, the Sensor monitors only the specified VLAN and ignores all other traffic.

Step 15 To enable/disable VLAN Filtering, click on the **Enable VLAN Filtering** checkbox in the heading bar.

Step 16 To specify the VLAN to be monitored, type its number in the text field.

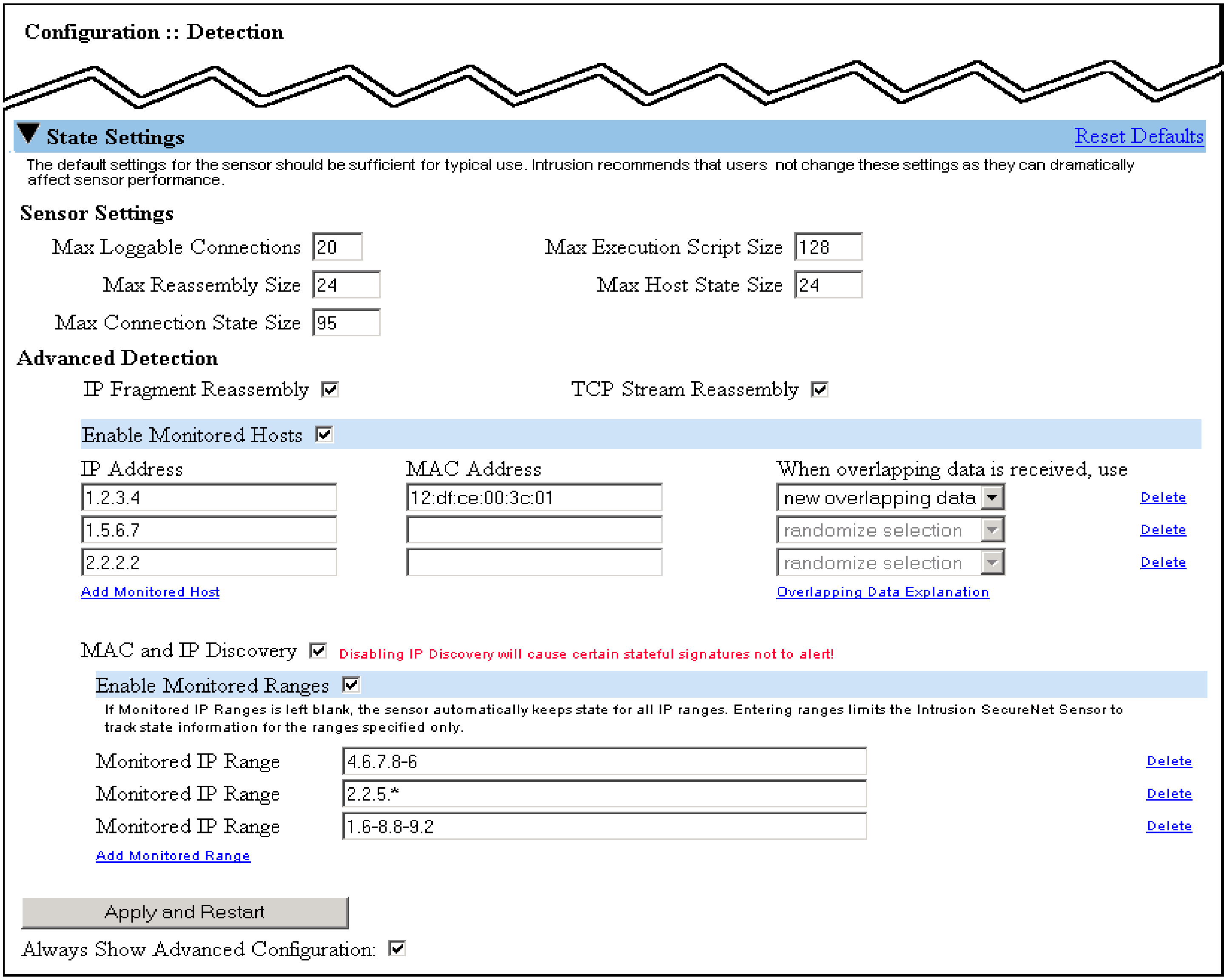
Step 17 When you have finished configuring the VLAN filtering, scroll down to the bottom of the page and click on the **Apply and Restart** button.

The Sensor restarts and begins monitoring the specified VLAN.

Configure State Settings

To view the current status of the SecureNet Sensor, perform the following steps:

Step 18 Scroll down the Detection Configuration page as needed to display the State Settings area shown in Figure 3-10.



Configuration :: Detection

▼ State Settings — Reset Defaults

The default settings for the sensor should be sufficient for typical use. Intrusion recommends that users not change these settings as they can dramatically affect sensor performance.

Sensor Settings

Max Loggable Connections: 20
Max Execution Script Size: 128
Max Reassembly Size: 24
Max Host State Size: 24
Max Connection State Size: 95

Advanced Detection

IP Fragment Reassembly ☑
TCP Stream Reassembly ☑

Enable Monitored Hosts ☑

IP Address	MAC Address	When overlapping data is received, use	
1.2.3.4	12:df:ce:00:3c:01	new overlapping data	Delete
1.5.6.7		randomize selection	Delete
2.2.2.2		randomize selection	Delete

Add Monitored Host
Overlapping Data Explanation

MAC and IP Discovery ☑ Disabling IP Discovery will cause certain stateful signatures not to alert!

Enable Monitored Ranges ☑

If Monitored IP Ranges is left blank, the sensor automatically keeps state for all IP ranges. Entering ranges limits the Intrusion SecureNet Sensor to track state information for the ranges specified only.

Monitored IP Range: 4.6.7.8-6 — Delete
Monitored IP Range: 2.2.5.* — Delete
Monitored IP Range: 1.6-8.8-9.2 — Delete

Add Monitored Range

Always Show Advanced Configuration: ☑

Figure 3-10 Detection Configuration Page (State Settings)

The State Settings area of the Detection Configuration page lets you select the Sensor settings and the advanced detection techniques that you want the Sensor to use. For definitions, refer to the *SecureNet Sensor Software User Guide* (formerly the *SecureNet Pro User Guide*).

Note The State Settings area has a **Reset Defaults** link that lets you set the options in this area to recommended factory default values. After setting to defaults, the values in the various fields are grayed. You can still edit the fields to values that you want.

Configure Sensor Settings

Step 19 To set the maximum number of loggable TCP connections that can be recorded simultaneously, type the number in the **Max Loggable Connections** field.

Step 20 To set the maximum number of megabytes of memory to be used by the fragmented IP packet reassembly subsystem, type the number in the **Max Reassembly Size** field.

Step 21 To set the maximum connection state size (in megabytes), type the number in the **Max Connection State Size** field.

Step 22 To set the maximum execution script size (in kilobytes), type the number in the **Max Execution Script Size** field.

Step 23 To set the maximum host state size (in megabytes), type the number in the **Max Host State Size** field.

Configure Advanced Detection

Step 24 To change the selection of any of the **Advanced Detection** options, click on the option's checkbox to select/deselect it.

Checked means that the option is to be used; unchecked means that the option is not to be used.

Configure Monitored Hosts

Step 25 To enable monitored hosts, click on the **Enable Monitored Hosts** checkbox to select it.

The list below the Enable Monitored Hosts checkbox shows the currently defined monitored hosts (if any).

Step 26 To add a monitored host, click on the **Add Monitored Host** link.

A set of text boxes display at the bottom of the list of defined monitored hosts. The right field (actually a pull-down list) is grayed out.

Step 27 In the left text box, specify the host's IP address and (optionally) type the host's MAC address in the center text box.

If you type a MAC address, the pull-down list for overlapping data handling becomes available.

Step 28 If you entered a MAC address, click on the arrow on the pull-down list for overlapping data and then select how you want overlapping data to be handled. The choices are **Randomize Selection** (default), **Old Overlapping Data**, and **New Overlapping Data**.

Note For an explanation of what overlapping data is and how it is handled, click on the **Overlapping Data Explanation** link below the list.

Step 29 To delete an existing monitored host from the list, click on the **Delete** link to the right of the host's entry in the list.

Configure Monitored Ranges

Step 30 To enable monitored ranges, click on the **Enable Monitored Ranges** checkbox to select it.

The list below the Enable Monitored Ranges checkbox shows the currently defined monitored ranges (if any).

Step 31 To add a monitored range, click on the **Add Monitored Ranges** link.

A text box displays at the bottom of the list of defined monitored ranges.

Step 32 In the text box, specify the IP address range using *dotted quad format*. Any quad can contain a range.

For example, you could type the range 123-212.

The new monitored range is added to the list.

Step 33 To delete an existing monitored range from the list, click on the **Delete** link to the right of the range's entry in the list. To delete a blank text box from the list, type any character in it and then click on the **Delete** link.

Note Enabling MAC and IP discovery lets the Sensor analyze network activity to automatically discover monitored MAC addresses and IP addresses. If disabled, some stateful signatures that should alert will be prevented from doing so.

Step 34 To enable MAC and IP discovery on the Sensor, click on the **MAC and IP Discovery** checkbox to select it.

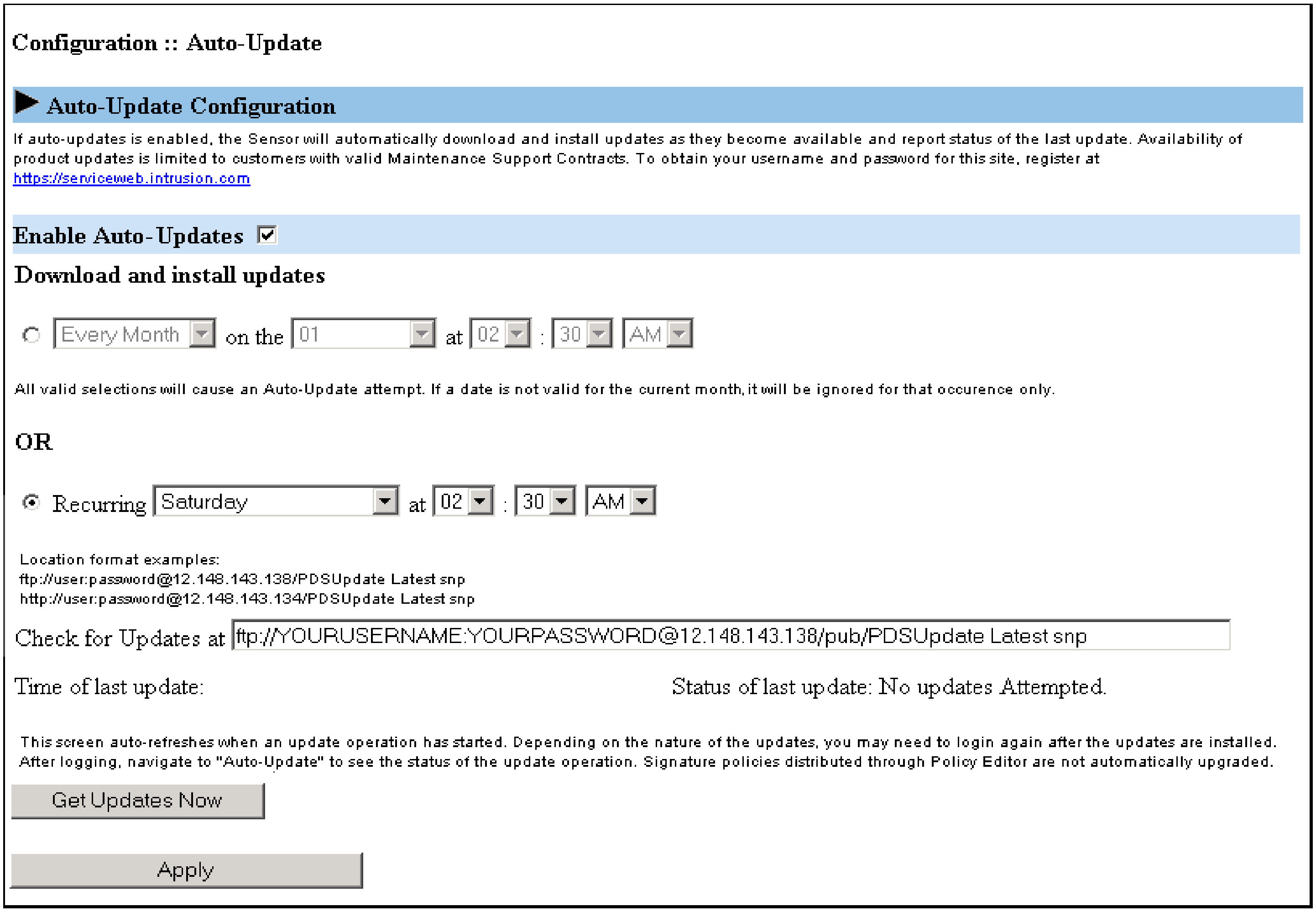
Step 35 Click on the **Apply and Restart** button to apply your changes and restart the Sensor.

Configure Auto-Update

To configure the SecureNet Sensor to automatically look for software updates and to install those updates when available, perform the following steps:

Step 1 At the top of any Intrusion SecureNet WBI page, click on the **Configuration** menu and then choose **Auto-Updates**.

The Auto-Update Configuration page displays (see Figure 3-11).



Configuration :: Auto-Update

▶ Auto-Update Configuration

If auto-updates is enabled, the Sensor will automatically download and install updates as they become available and report status of the last update. Availability of product updates is limited to customers with valid Maintenance Support Contracts. To obtain your username and password for this site, register at https://serviceweb.intrusion.com

Enable Auto-Updates ☑

Download and install updates

○ Every Month on the 01 at 02 : 30 AM

All valid selections will cause an Auto-Update attempt. If a date is not valid for the current month, it will be ignored for that occurence only.

OR

● Recurring Saturday at 02 : 30 AM

Location format examples:
ftp://user:password@12.148.143.138/PDSUpdate Latest snp
http://user:password@12.148.143.134/PDSUpdate Latest snp

Check for Updates at ftp://YOURUSERNAME:YOURPASSWORD@12.148.143.138/pub/PDSUpdate Latest snp

Time of last update:

Status of last update: No updates Attempted.

This screen auto-refreshes when an update operation has started. Depending on the nature of the updates, you may need to login again after the updates are installed. After logging, navigate to "Auto-Update" to see the status of the update operation. Signature policies distributed through Policy Editor are not automatically upgraded.

Figure 3-11 Auto-Update Configuration Page

This page lets you enable automatic updating of the SecureNet Sensor software, lets you choose the frequency at which the system looks for any available updates, and lets you specify where to look for updates. After each attempt at automatic updating, this page displays the time, date, and status of the update.

Step 2 To enable automatic updating of software, click on the **Enable Auto Updates** checkbox to select it.

Step 3 To set the frequency at which the system is to look for updates, click on one of the two radio buttons and then choose the frequency using the pull-down lists:

- Periodic—Lets you choose to have the system automatically look for software updates on a specified day at a specified time on:
  - Every Month
  - Even Months
  - Odd Months
  - A specific month
  - Every other month
- Recurring—Lets you choose to have the system automatically look for software updates at a specified time on:
  - Every Day
  - Every Weekday
  - Specified days

Important! Intrusion’s downloadable software files are now available from ServiceWeb, a members-only FTP site reserved for customers who have maintenance agreements with Intrusion Inc. If you do not have a membership, you must go to https://serviceweb.intrusion.com/request.asp to complete and submit an Access Authorization Request form.

When your Access Authorization Request is approved, emails will be sent to the addresses you provided for the Primary Contact and the Secondary Contact. You can then use your ServiceWeb Username and Password when performing software upgrades as described in this procedure.

Step 4 In the **Check for Updates at** field, type

ftp://<*yourusername*>:<*yourpassword*>@12.148.143.138/pub/PDSUpdate Latest snp
(Be sure to enter the spaces before and after the word “Latest”.)

Step 5 When you have completed your selections and entered a valid location, click on the **Get Updates Now** button to check for updates now (regardless of the frequency settings)
-OR-
Click on **Apply** button to save your changes.

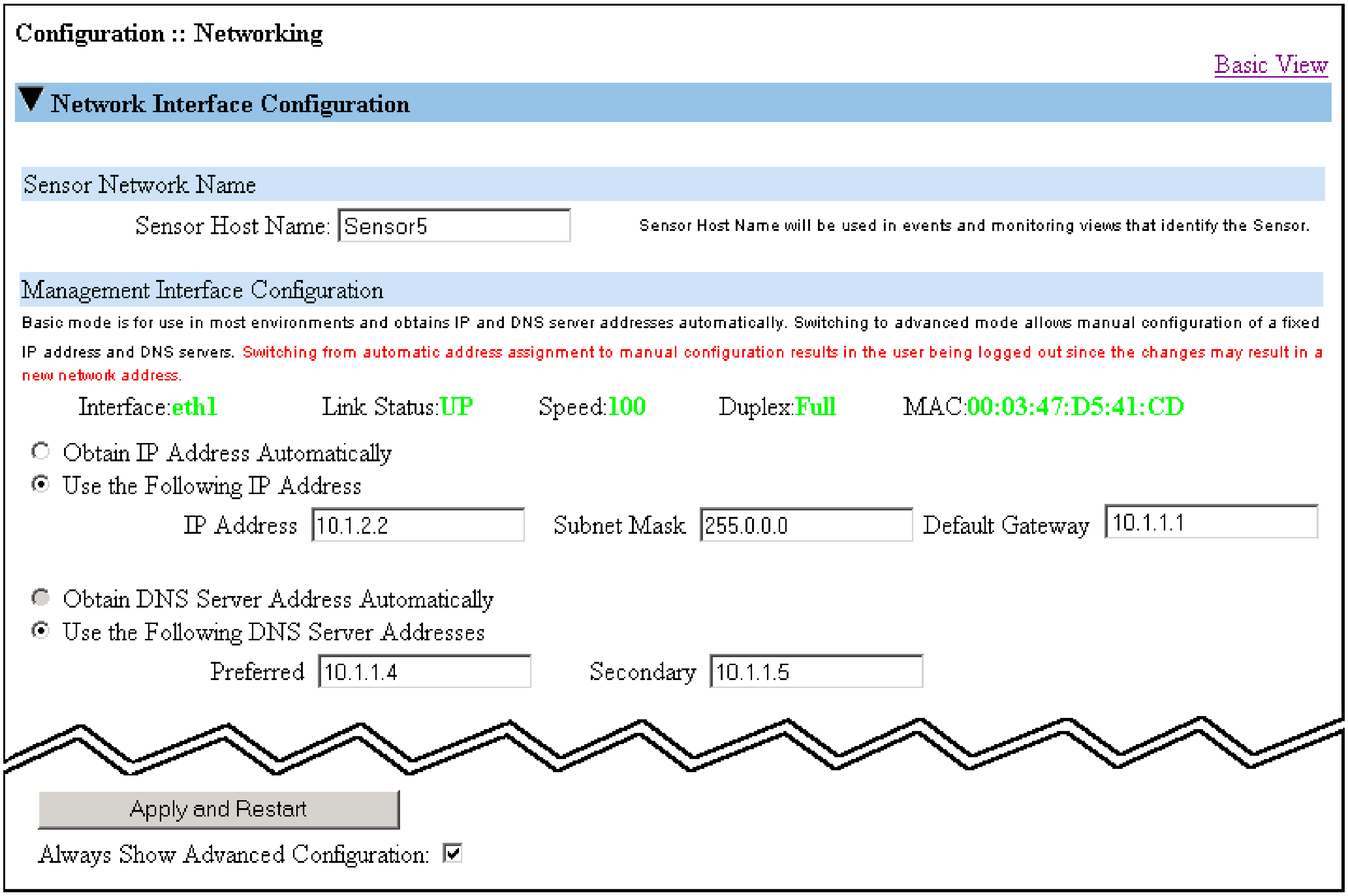
The system checks for updates as specified and, if updates are available, it downloads and installs them. Upon completion, the **Time of Last Update** and **Status** fields are refreshed with current data.

Configure Networking

To configure networking parameters for the Sensor, perform the following steps:

Step 1 At the top of any Intrusion SecureNet WBI page, click on the **Configuration** menu and then choose **Networking**.

The Networking Configuration page displays (see Figure 3-12).



Configuration :: Networking

Basic View

▼ **Network Interface Configuration**

Sensor Network Name

Sensor Host Name: Sensor5 — Sensor Host Name will be used in events and monitoring views that identify the Sensor.

Management Interface Configuration

Basic mode is for use in most environments and obtains IP and DNS server addresses automatically. Switching to advanced mode allows manual configuration of a fixed IP address and DNS servers. Switching from automatic address assignment to manual configuration results in the user being logged out since the changes may result in a new network address.

Interface:**eth1** Link Status:**UP** Speed:**100** Duplex:**Full** MAC:**00:03:47:D5:41:CD**

○ Obtain IP Address Automatically

● Use the Following IP Address

IP Address: 10.1.2.2 Subnet Mask: 255.0.0.0 Default Gateway: 10.1.1.1

○ Obtain DNS Server Address Automatically

● Use the Following DNS Server Addresses

Preferred: 10.1.1.4 Secondary: 10.1.1.5

Apply and Restart

Always Show Advanced Configuration: ☑

Figure 3-12 Networking Configuration (Management Interface) Page

Assign Sensor Host Name

Important! In the following step, you should apply a unique Sensor Host Name to the Sensor, especially if you plan on configuring multiple Sensors for your network. Each Sensor *must* have a unique Host Name.

Step 2 In the **Sensor Host Name** field, type the hostname that you want to assign to the Sensor.

View Management Interface Status

The Management Interface section of the Networking Configuration page lets you view the current status of the Management Interface (*eth1*) using read-only fields in colors that help you determine its state at a glance. **Green** items indicate favorable status; **Red** items indicate unfavorable status. The **Interface** field shows the interface that is currently assigned management (usually *eth1*). The **Link Status** field indicates whether the interface is currently **Up** (working) or **Down** (not working). The **Speed** field indicates the interface's maximum speed in megabits-per-second (Mbps or Mb/s). The **Duplex** field shows whether the interface is operating at half-duplex or full-duplex. The **MAC** field displays the interface's Media Access Control (MAC) address, your Sensor's unique hardware number.

Configure Management Interface

The Networking Configuration page lets you specify whether the interface's IP address should be dynamically assigned upon the Sensor being booted or it should use a specified static IP address. It also lets you specify whether the interface's DNS server address should be dynamically assigned upon boot or it should use one of two specified static addresses.

Note Automatic configuration of the management interface IP address can be done only if a DHCP server is available or reachable on the network.

Step 3 If you want to have the interface's IP address be dynamically assigned upon the Sensor being booted, click on the **Obtain IP Address Automatically** radio button to select it and then go to Step 5.
-OR-
If you want to specify the IP address that is to be used, perform the following steps:

a. Click on the **Use the Following IP Address** radio button to select it.

b. In the **IP Address** field, enter the interface's static IP address using dotted quad format.

c. In the **Subnet Mask** field, enter the interface's subnet mask using dotted quad format.

d. In the **Default Gateway** field, enter the default gateway's hostname or IP address in dotted quad format.

Note If you want to have the Sensor to get the DNS server address automatically, any changes to the Sensor's Host Name will be propagated into the network using the NetBIOS name server.

Step 4 If you want to have the interface's Domain Name Server (DNS) address be dynamically assigned upon the Sensor being booted, click on the **Obtain DNS Server Address Automatically** radio button to select it and then go to Step 5.
-OR-
If you want to specify the Preferred and Secondary IP address that are to be used, perform the following steps:

a. Click on the **Use the Following DNS Server Addresses** radio button to select it.

b. In the **Preferred** field, enter the preferred DNS's static IP address using dotted quad format.

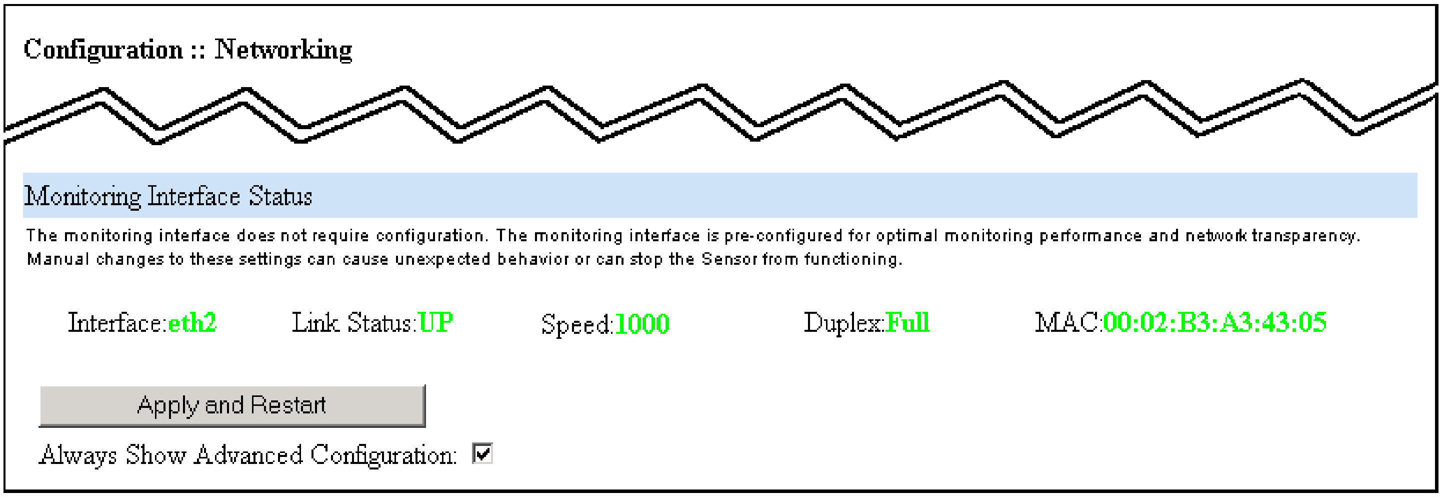
c. *(Optional)* In the **Secondary** field, enter a secondary DNS's static IP address using dotted quad format.

Step 5 To apply your changes and restart the Sensor so that they take effect, scroll to the bottom of the page and click on the **Apply and Restart** button.

The management interface configuration changes are applied to the Sensor and the SecureNet WBI login page displays.

View Monitoring Interface Status

Step 6 To view the status of the Monitoring Interface, scroll to the bottom of the Networking Configuration page (see Figure 3-13).



Configuration :: Networking

Monitoring Interface Status

The monitoring interface does not require configuration. The monitoring interface is pre-configured for optimal monitoring performance and network transparency. Manual changes to these settings can cause unexpected behavior or can stop the Sensor from functioning.

Interface:eth2 Link Status:UP Speed:1000 Duplex:Full MAC:00:02:B3:A3:43:05

Always Show Advanced Configuration: ☑

Figure 3-13 Networking Configuration (Monitoring Interface) Page

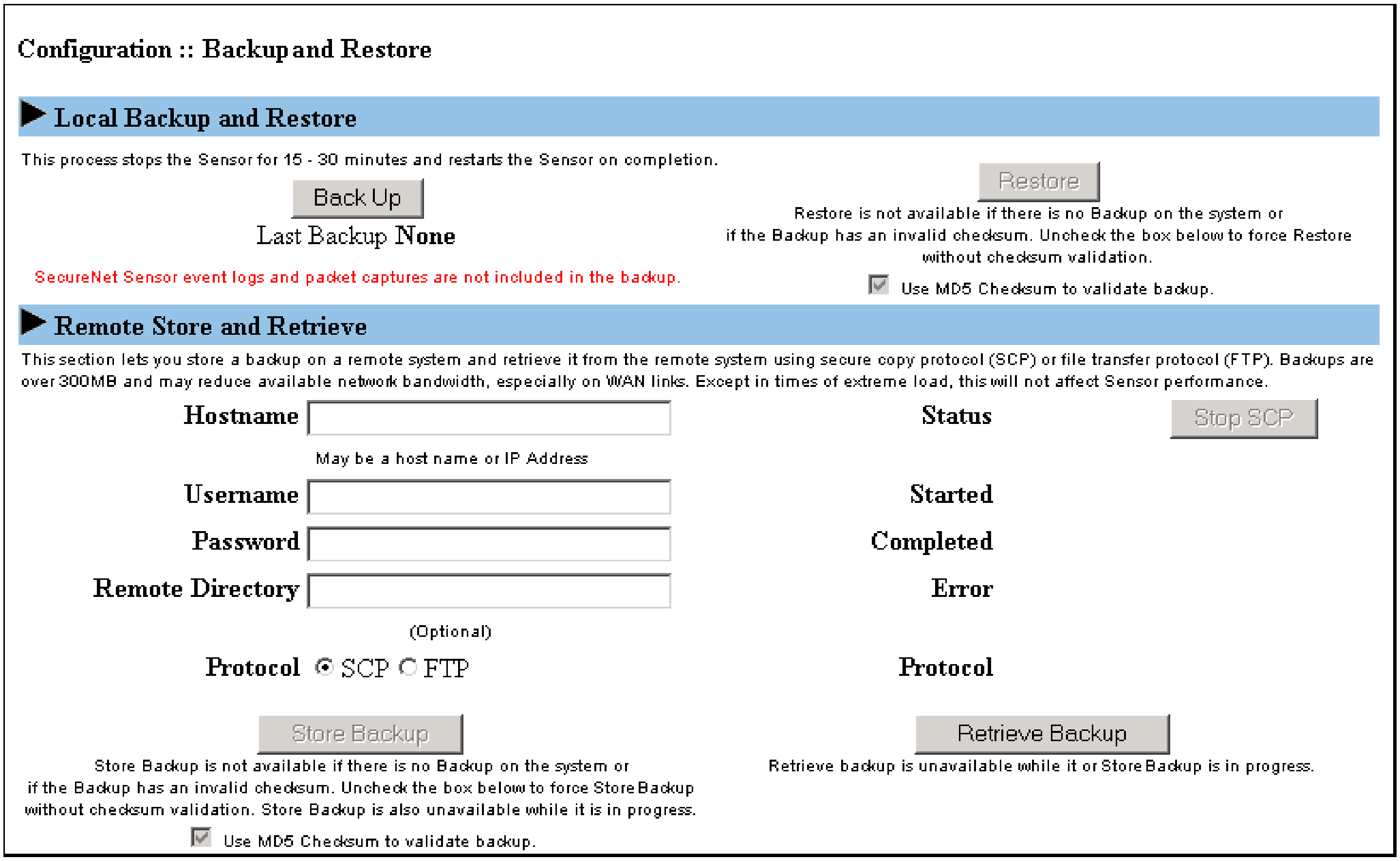
The Monitoring Interface section of the Networking Configuration page lets you view the current status of the Monitoring Interface (in this case *eth2*) using read-only fields in colors that help you determine its state at a glance. **Green** items indicate favorable status; **Red** items indicate unfavorable status. The **Interface** field shows the interface that is currently assigned management (usually *eth2*). The **Link Status** field indicates whether the interface is currently **Up** (working) or **Down** (not working). The **Speed** field indicates the interface's maximum speed in megabits-per-second (Mbps or Mb/s). The **Duplex** field shows whether the interface is operating at half-duplex or full-duplex. The **MAC** field displays the interface's Media Access Control (MAC) address, your Sensor's unique hardware number.

Configure Backup and Restore Options

To back up and restore your Sensor, perform the following steps:

Step 1 At the top of any Intrusion SecureNet WBI page, click on the **Configuration** menu and then choose **Backup/Restore**.

The Backup and Restore Configuration page displays (see Figure 3-14).



Configuration :: Backup and Restore

▶ Local Backup and Restore

This process stops the Sensor for 15 - 30 minutes and restarts the Sensor on completion.

Last Backup None

SecureNet Sensor event logs and packet captures are not included in the backup.

Restore is not available if there is no Backup on the system or if the Backup has an invalid checksum. Uncheck the box below to force Restore without checksum validation.

☑ Use MD5 Checksum to validate backup.

▶ Remote Store and Retrieve

This section lets you store a backup on a remote system and retrieve it from the remote system using secure copy protocol (SCP) or file transfer protocol (FTP). Backups are over 300MB and may reduce available network bandwidth, especially on WAN links. Except in times of extreme load, this will not affect Sensor performance.

Hostname

May be a host name or IP Address

Username

Password

Remote Directory

(Optional)

Protocol ● SCP ○ FTP

Status

Started

Completed

Error

Protocol

Store Backup is not available if there is no Backup on the system or if the Backup has an invalid checksum. Uncheck the box below to force Store Backup without checksum validation. Store Backup is also unavailable while it is in progress.

☑ Use MD5 Checksum to validate backup.

Retrieve backup is unavailable while it or Store Backup is in progress.

Figure 3-14 Backup and Restore Configuration Page

Note The figure above shows how the Backup and Restore page looks before any backups have been performed.

This page lets you perform backups of the sensor system files and lets you restore the files on your Sensor in the event of a data loss or corruption. It also lets you store a copy of the backup at a remote location for later retrieval. Remote Store and Retrieve processes can be performed using FTP (file transfer protocol) or SCP (secure copy, a method of copying data from one system to another over a network using a secure (encrypted) connection).

The steps for performing these tasks are given in the following sections:

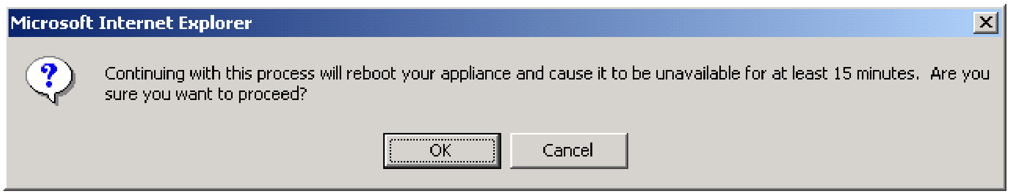
"Back Up System Files" on page 3-24
"Restore from Local Backup" on page 3-25
"Store Backup at Remote Location" on page 3-26
"Retrieve Backup From Remote Storage" on page 3-28

Back Up System Files

Note There can be only one local backup on the system. When you create a new backup, any existing backup is overwritten.

Step 2 Click on the **Back Up** button.

The following warning message displays:



Microsoft Internet Explorer

Continuing with this process will reboot your appliance and cause it to be unavailable for at least 15 minutes. Are you sure you want to proceed?

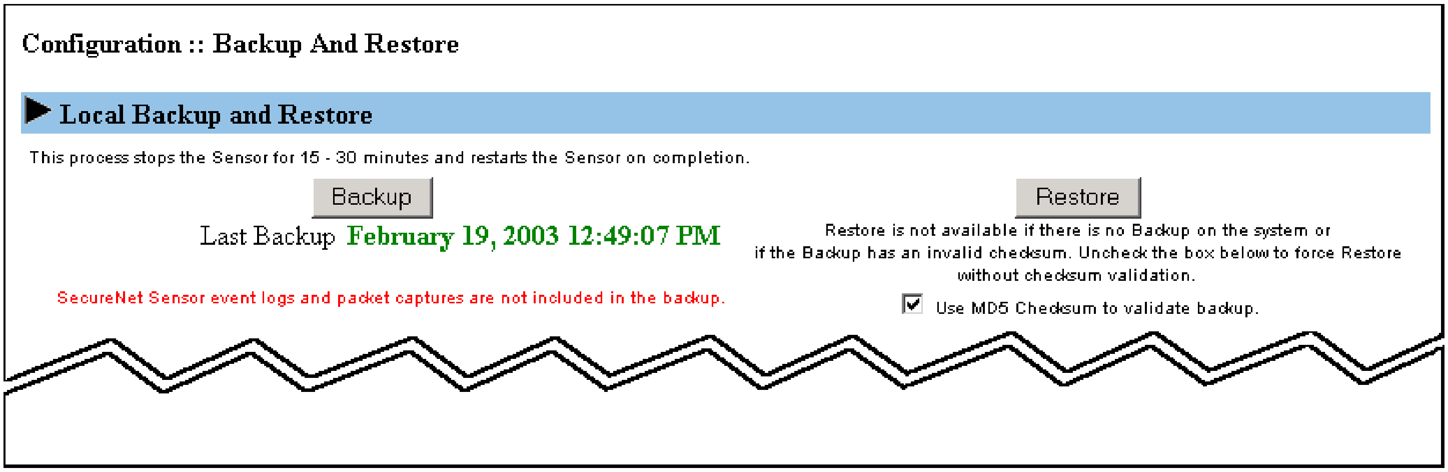
Step 3 Click on **OK** to continue.

The Backup process begins. Remember that your Sensor and SecureNet WBI will be unavailable during the time that it takes to perform the backup. At the completion of the Backup process, the Sensor is restarted and SecureNet WBI is available again.

Step 4 Wait for the Backup process to complete and try to log in to the SecureNet WBI again. Because the backup time is indefinite, you may need to try logging in several times before you are successful.

Step 5 Click on the **Configuration** menu and then choose **Backup/Restore**.

The Backup and Restore Configuration page displays (see Figure 3-15).



Configuration :: Backup And Restore

▶ Local Backup and Restore

This process stops the Sensor for 15 - 30 minutes and restarts the Sensor on completion.

Last Backup February 19, 2003 12:49:07 PM

Restore is not available if there is no Backup on the system or if the Backup has an invalid checksum. Uncheck the box below to force Restore without checksum validation.

SecureNet Sensor event logs and packet captures are not included in the backup.

☑ Use MD5 Checksum to validate backup.

Figure 3-15 Backup/Restore Configuration Page (Local Backup/Restore)

Notice that the Restore button is made available and the date on which the Last Backup was performed is shown. If the last backup failed due to an integrity problem, the Restore button would be unavailable and the following text would be displayed instead:

Last Backup **Checksum Failed**

Restore from Local Backup

Note If the Restore button is unavailable, it may be due to the Sensor not having a backup stored locally or the inability to verify the integrity of backup stored locally on the Sensor.

If the Restore button is unavailable because of the inability to verify the backup's integrity, you can override the integrity requirement by clicking on the **Use MD5 Checksum to validate backup** checkbox to uncheck it. This lets you restore the system from a backup even if its MD5 checksum cannot be validated.

Step 6 Click on the **Restore** button.

The Restore process begins. Remember that the Sensor and SecureNet WBI will be unavailable during the time that it takes to perform the restore. At the completion of the Restore process, the Sensor is restarted and SecureNet WBI is available again.

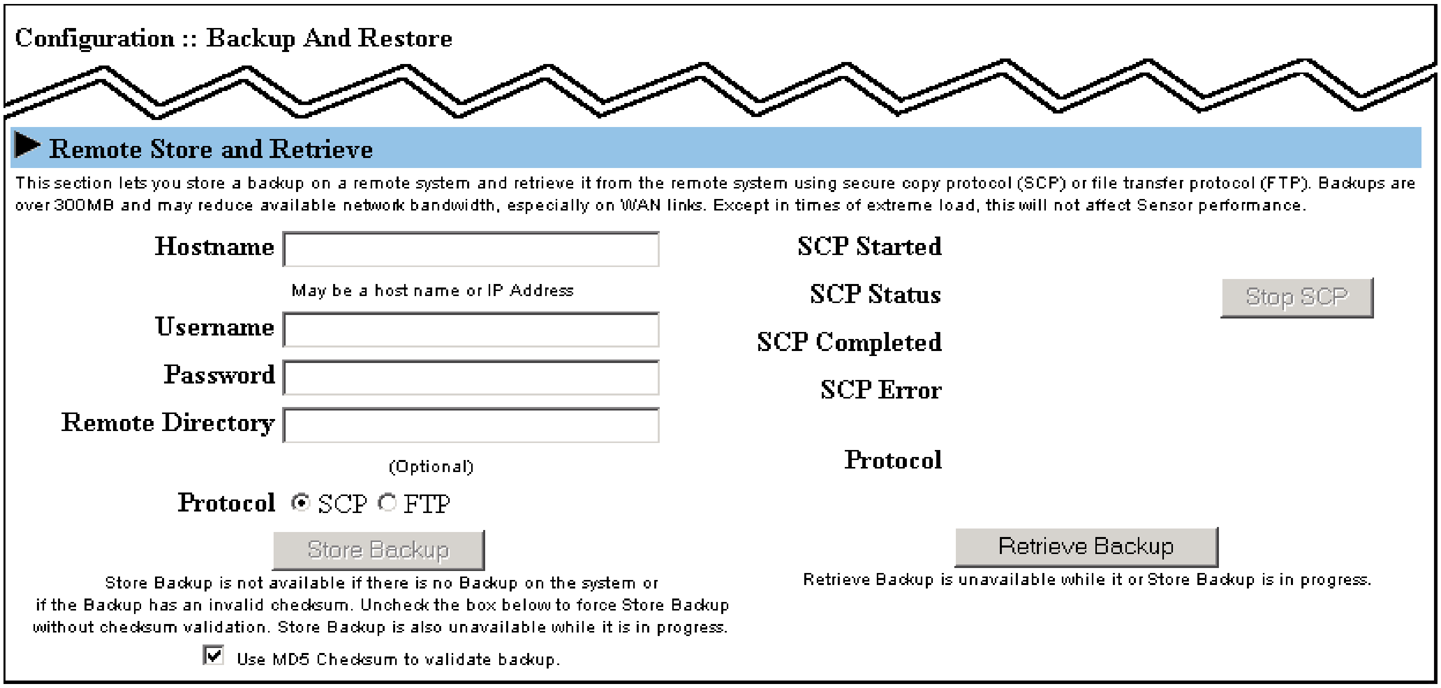
Step 7 Wait for the Restore process to complete and try to log in to the SecureNet WBI again. Because the restoration time is indefinite, you may need to try logging in several times before you are successful.

There is currently no method of using the SecureNet WBI to determine whether the restoration was successful other than your ability to successfully log in to SecureNet WBI.

Store Backup at Remote Location

Note If you do not have a valid backup, the Store Backup button is not available.

Step 8 Scroll the Backup and Restore Configuration page to show the lower area of the page (see Figure 3-16).



Configuration :: Backup And Restore

▶ Remote Store and Retrieve

This section lets you store a backup on a remote system and retrieve it from the remote system using secure copy protocol (SCP) or file transfer protocol (FTP). Backups are over 300MB and may reduce available network bandwidth, especially on WAN links. Except in times of extreme load, this will not affect Sensor performance.

Hostname

May be a host name or IP Address

Username

Password

Remote Directory

(Optional)

Protocol ● SCP ○ FTP

Store Backup is not available if there is no Backup on the system or if the Backup has an invalid checksum. Uncheck the box below to force Store Backup without checksum validation. Store Backup is also unavailable while it is in progress.

☑ Use MD5 Checksum to validate backup.

SCP Started

SCP Status

SCP Completed

SCP Error

Protocol

Retrieve Backup is unavailable while it or Store Backup is in progress.

Figure 3-16 Backup/Restore Configuration Page (Remote Store/Retrieve)

Step 9 In the **Hostname** field, type the IP address (in dotted quad format) or the domain name of the remote location where the backup is to be stored. Do not use any protocol prefixes (such as http:// or ftp://) or any directory path information in this field.

Step 10 In the **Username** field, type the username to be used to authenticate on the remote host. If the domain accepts anonymous logins, you can leave this field blank.

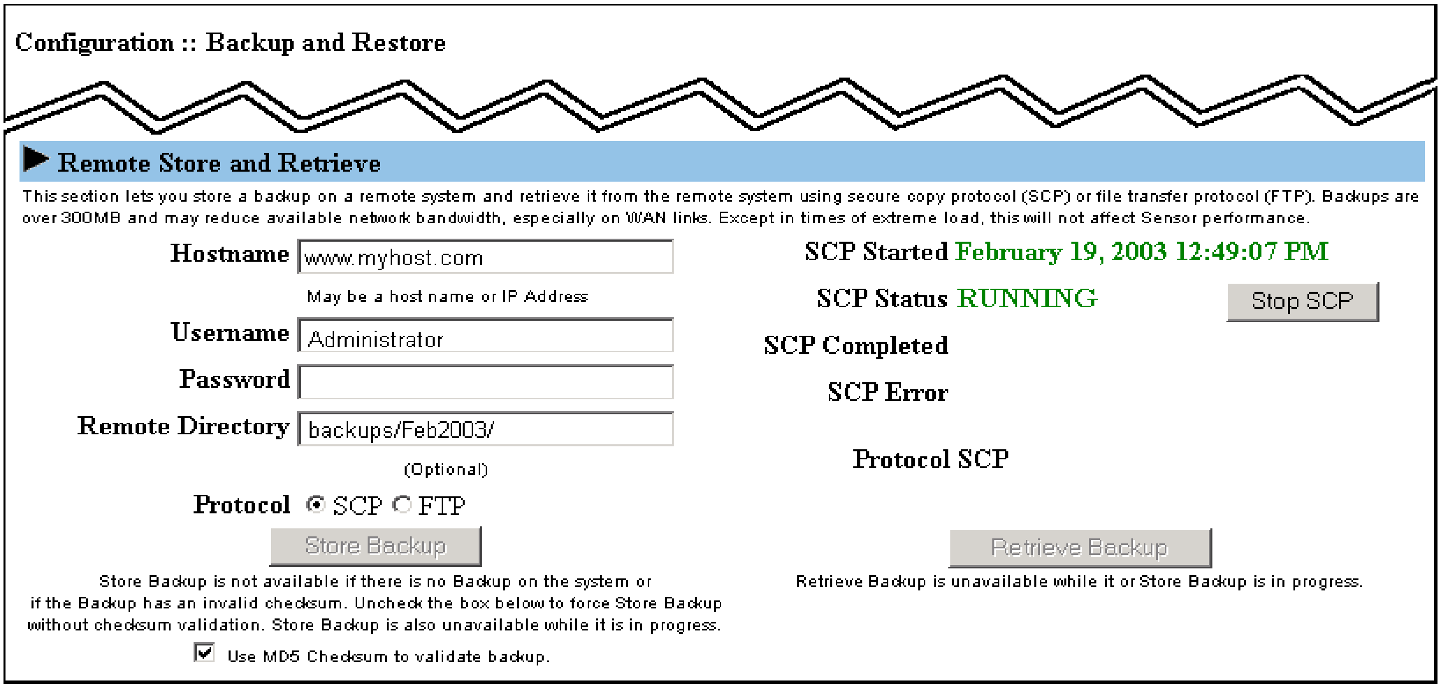
Step 11 In the **Password** field, type the password to be used to authenticate on the remote host. If the domain accepts anonymous logins, you can leave this field blank.

Step 12 In the **Remote Directory** field, type the path to the directory on the host where you want the backup stored.

Step 13 Click on the **Protocol** radio button for the method of transfer that you want to be used.

Step 14 Click on the **Store Backup** button.

The Remote Store process begins running in the background. The Backup and Restore Configuration page displays the start time and shows the status as **RUNNING** (see Figure 3-17).



Configuration :: Backup and Restore

▶ Remote Store and Retrieve

This section lets you store a backup on a remote system and retrieve it from the remote system using secure copy protocol (SCP) or file transfer protocol (FTP). Backups are over 300MB and may reduce available network bandwidth, especially on WAN links. Except in times of extreme load, this will not affect Sensor performance.

Hostname www.myhost.com

May be a host name or IP Address

Username Administrator

Password

Remote Directory backups/Feb2003/

(Optional)

Protocol ● SCP ○ FTP

Store Backup is not available if there is no Backup on the system or if the Backup has an invalid checksum. Uncheck the box below to force Store Backup without checksum validation. Store Backup is also unavailable while it is in progress.

☑ Use MD5 Checksum to validate backup.

SCP Started February 19, 2003 12:49:07 PM

SCP Status RUNNING

SCP Completed

SCP Error

Protocol SCP

Retrieve Backup is unavailable while it or Store Backup is in progress.

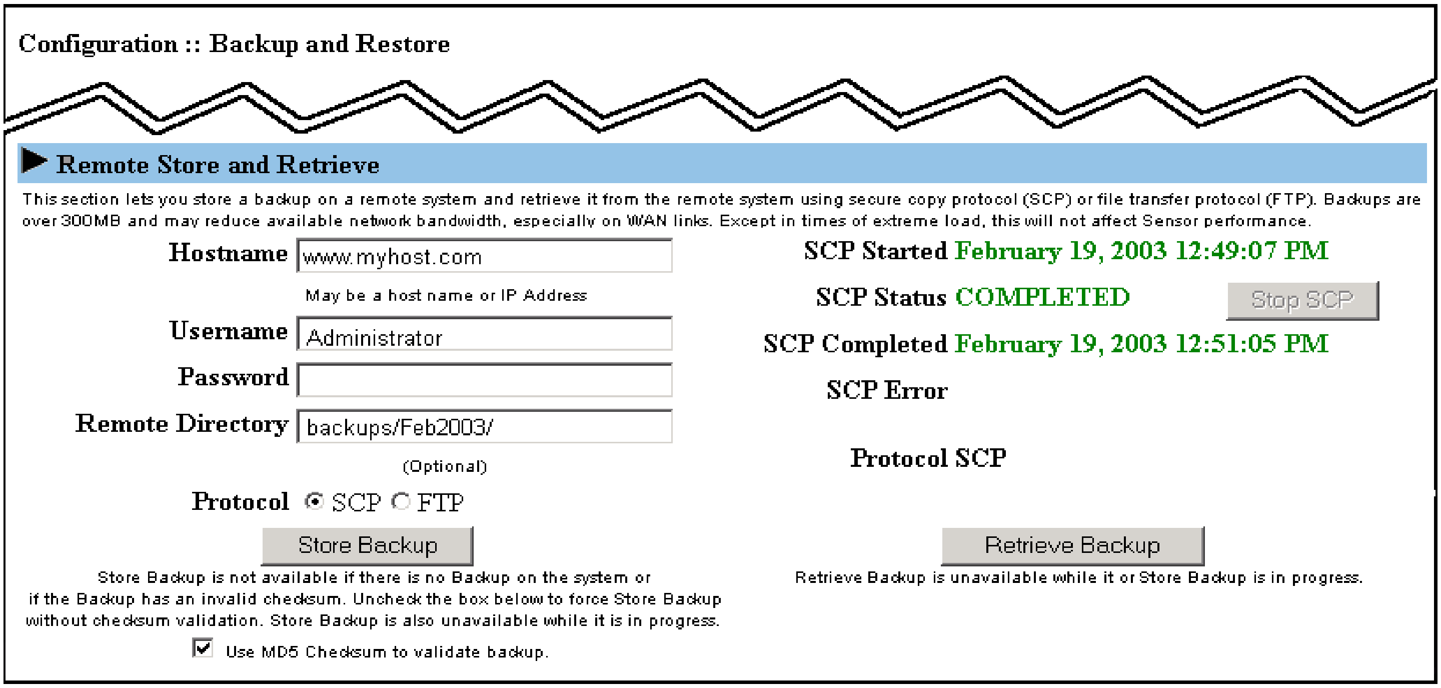
Figure 3-17 Backup/Restore Configuration Page (Remote Store Running)

The Sensor availability is not affected while the transfer is being done. The Remote Store process may take a long time to complete, depending on the available bandwidth on the network.

Note If you need to stop the Remote Store process from running, click on the **Stop SCP/FTP** button. The process is stopped unconditionally, therefore the remote backup will likely not be usable due to its being partially overwritten.

Step 15 Wait for the Remote Store process to complete.

When the process is completed successfully, the Backup and Restore Configuration page displays the status as **COMPLETED** and the date/time (see Figure 3-18).



Configuration :: Backup and Restore

▶ Remote Store and Retrieve

This section lets you store a backup on a remote system and retrieve it from the remote system using secure copy protocol (SCP) or file transfer protocol (FTP). Backups are over 300MB and may reduce available network bandwidth, especially on WAN links. Except in times of extreme load, this will not affect Sensor performance.

Hostname www.myhost.com

May be a host name or IP Address

Username Administrator

Password

Remote Directory backups/Feb2003/

(Optional)

Protocol ● SCP ○ FTP

Store Backup is not available if there is no Backup on the system or if the Backup has an invalid checksum. Uncheck the box below to force Store Backup without checksum validation. Store Backup is also unavailable while it is in progress.

☑ Use MD5 Checksum to validate backup.

SCP Started February 19, 2003 12:49:07 PM

SCP Status COMPLETED

SCP Completed February 19, 2003 12:51:05 PM

SCP Error

Protocol SCP

Retrieve Backup is unavailable while it or Store Backup is in progress.

Figure 3-18 Backup/Restore Configuration Page (Store Completed)

Retrieve Backup From Remote Storage

Note There can be only one local backup on the system. When you retrieve a backup from remote storage, it overwrites the existing local backup.

Step 16 On the Backup and Restore Configuration page (see Figure 3-17), type the password for the remote host in the **Password** field.

Step 17 If necessary, in the **Hostname** field, type the IP address (in dotted quad format) or the domain name of the remote location where the backup was remotely stored.

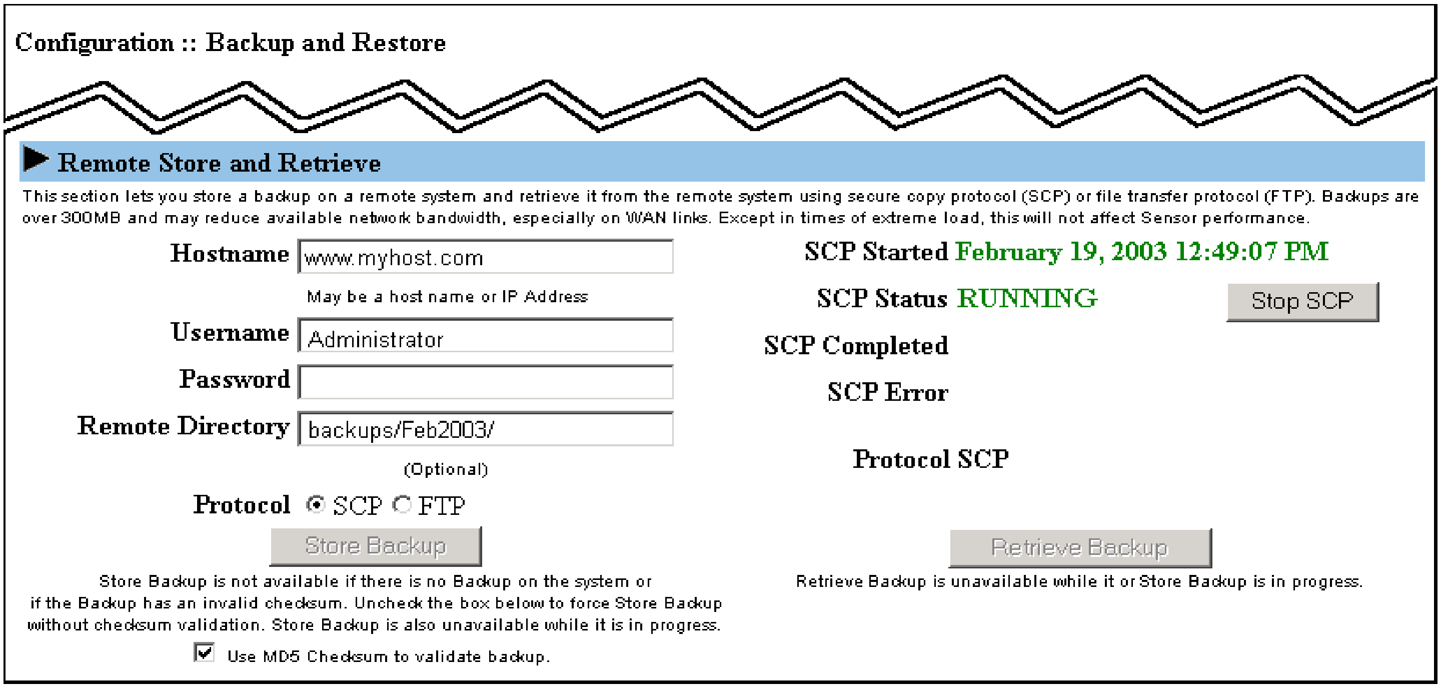
Step 18 If necessary, in the **Username** field, type the username to be used to authenticate on the remote host. If the domain accepts anonymous logins, you can leave this field blank.

Step 19 If necessary, in the **Remote Directory** field, type the path to the directory on the host where the backup was remotely stored.

Step 20 Click on the **Protocol** radio button for the method of transfer that you want to be used.

Step 21 Click on the **Retrieve Backup** button.

The Remote Retrieve process begins running in the background. The Backup and Restore Configuration page displays the start time and shows the status as **RUNNING** (see Figure 3-19).



Configuration :: Backup and Restore

▶ Remote Store and Retrieve

This section lets you store a backup on a remote system and retrieve it from the remote system using secure copy protocol (SCP) or file transfer protocol (FTP). Backups are over 300MB and may reduce available network bandwidth, especially on WAN links. Except in times of extreme load, this will not affect Sensor performance.

Hostname: www.myhost.com
May be a host name or IP Address

Username: Administrator

Password:

Remote Directory: backups/Feb2003/
(Optional)

Protocol ● SCP ○ FTP

SCP Started February 19, 2003 12:49:07 PM

SCP Status RUNNING

SCP Completed

SCP Error

Protocol SCP

Store Backup is not available if there is no Backup on the system or if the Backup has an invalid checksum. Uncheck the box below to force Store Backup without checksum validation. Store Backup is also unavailable while it is in progress.

☑ Use MD5 Checksum to validate backup.

Retrieve Backup is unavailable while it or Store Backup is in progress.

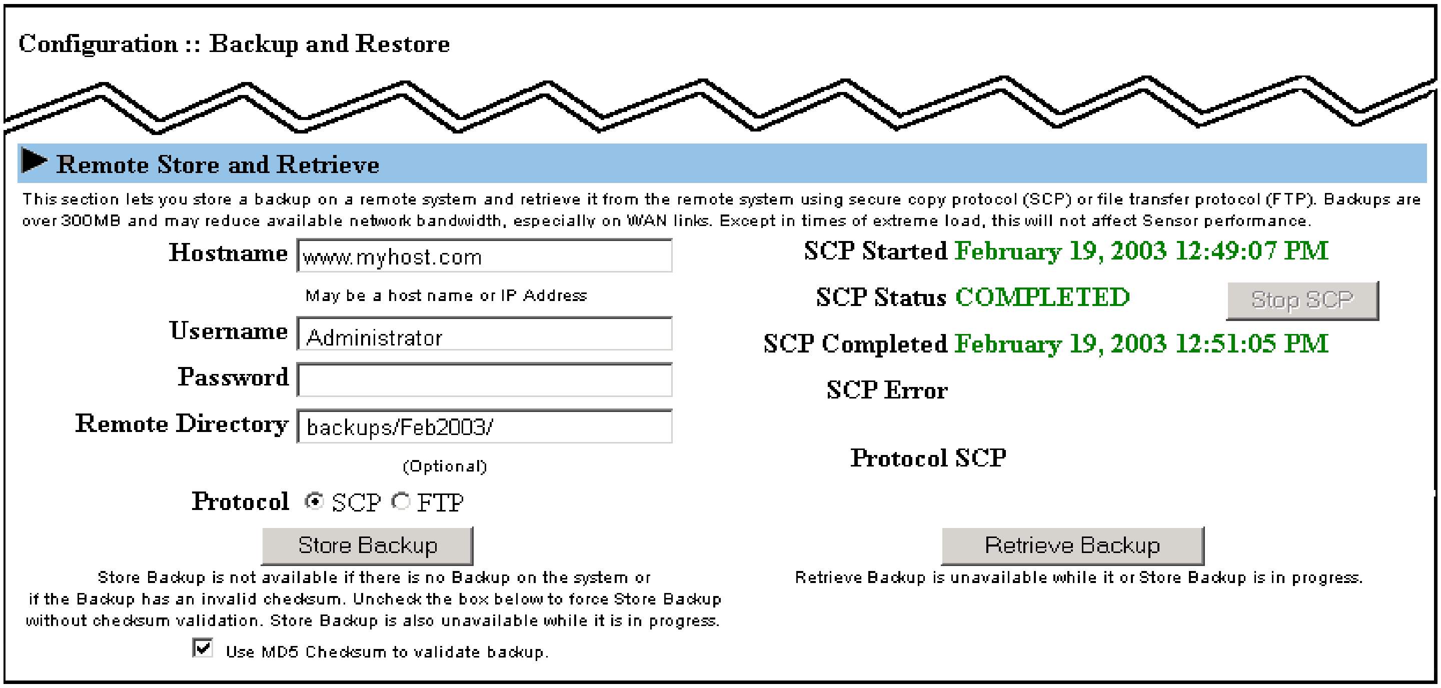
Figure 3-19 Backup/Restore Configuration Page (Retrieve Running)

The Sensor availability is not affected while the transfer is being done. The Remote Retrieve process may take a long time to complete, depending on the available bandwidth on the network.

Note If you need to stop the Remote Retrieve process from running, click on the **Stop SCP/FTP** button. The process is stopped unconditionally, therefore the local backup will likely not be usable due to its being partially overwritten.

Step 22 Wait for the Remote Retrieve process to complete.

When the process is completed successfully, the Backup and Restore Configuration page displays the status as **COMPLETED** and the date/time (see Figure 3-20).



Configuration :: Backup and Restore

▶ Remote Store and Retrieve

This section lets you store a backup on a remote system and retrieve it from the remote system using secure copy protocol (SCP) or file transfer protocol (FTP). Backups are over 300MB and may reduce available network bandwidth, especially on WAN links. Except in times of extreme load, this will not affect Sensor performance.

Hostname: www.myhost.com
May be a host name or IP Address

Username: Administrator

Password:

Remote Directory: backups/Feb2003/
(Optional)

Protocol ● SCP ○ FTP

Store Backup is not available if there is no Backup on the system or if the Backup has an invalid checksum. Uncheck the box below to force Store Backup without checksum validation. Store Backup is also unavailable while it is in progress.

☑ Use MD5 Checksum to validate backup.

SCP Started February 19, 2003 12:49:07 PM

SCP Status COMPLETED

SCP Completed February 19, 2003 12:51:05 PM

SCP Error

Protocol SCP

Retrieve Backup is unavailable while it or Store Backup is in progress.

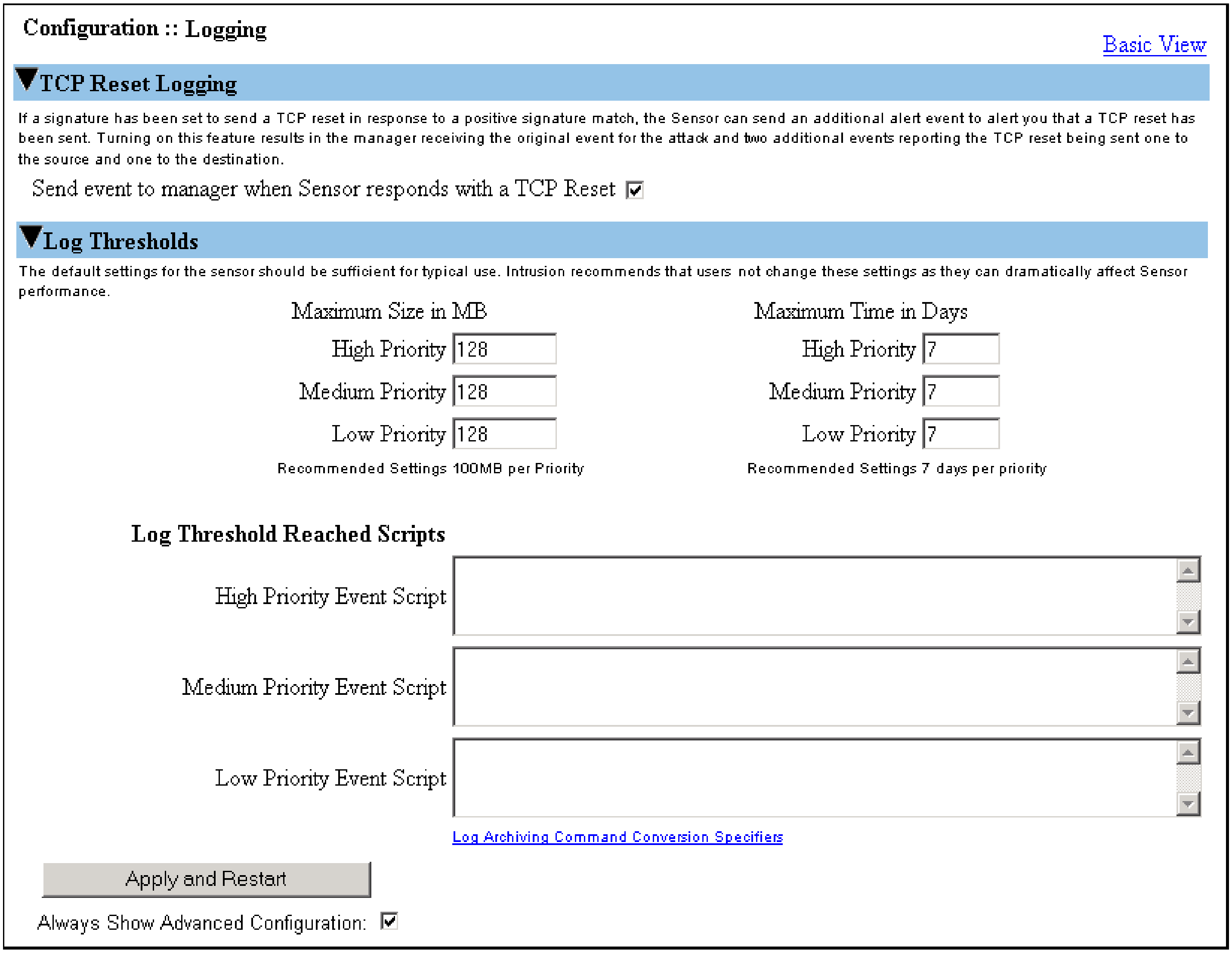
Figure 3-20 Backup/Restore Configuration Page (Retrieve Completed)

Configure Logging Options

To configure the event logging options for the SecureNet Sensor, perform the following steps:

Step 1 At the top of any Intrusion SecureNet WBI page, click on the **Configuration** menu and then choose **Logging**.

The Event Logging Configuration page displays as shown in Figure 3-21.



Configuration :: Logging

Basic View

TCP Reset Logging

If a signature has been set to send a TCP reset in response to a positive signature match, the Sensor can send an additional alert event to alert you that a TCP reset has been sent. Turning on this feature results in the manager receiving the original event for the attack and two additional events reporting the TCP reset being sent one to the source and one to the destination.

Send event to manager when Sensor responds with a TCP Reset ☑

Log Thresholds

The default settings for the sensor should be sufficient for typical use. Intrusion recommends that users not change these settings as they can dramatically affect Sensor performance.

Maximum Size in MB		Maximum Time in Days	
High Priority	128	High Priority	7
Medium Priority	128	Medium Priority	7
Low Priority	128	Low Priority	7
Recommended Settings 100MB per Priority		Recommended Settings 7 days per priority	

Log Threshold Reached Scripts

High Priority Event Script

Medium Priority Event Script

Low Priority Event Script

Log Archiving Command Conversion Specifiers

Apply and Restart

Always Show Advanced Configuration: ☑

Figure 3-21 Event Logging Configuration Page

The Event Logging Configuration page lets you set the maximum size (in megabytes) based on the priority of the record and the maximum age (in number of days old) of the records that are to be retained in the log.

Step 2 In the **Maximum Size in MB** column, type the maximum amount of disk space to be used for records of different priorities. When the records in a priority reaches its maximum disk size, older records are purged from the logs to provide space needed for new records.

Step 3 In the **Maximum Time in Days** column, type the maximum age (in number of days old) of the records that are to be retained in the log. When a record reaches its maximum age, it is purged from the logs.

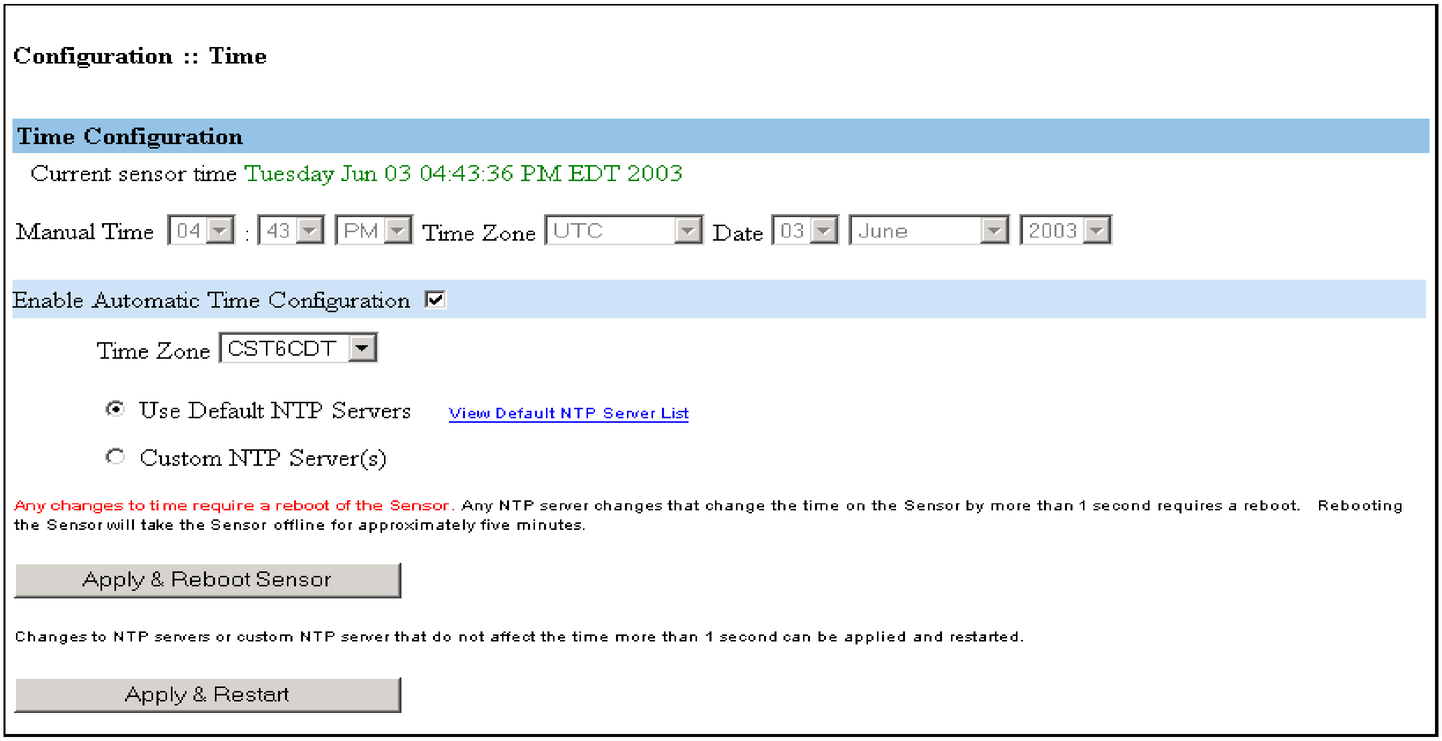
Step 4 When you have finished making changes, click on the **Apply and Restart** button to apply your changes and restart the Sensor.

Configure Time Options

To configure the Time settings for the Sensor, perform the following steps:

Step 1 At the top of any Intrusion SecureNet WBI page, click on the **Configuration** menu and then choose **Time**.

The Time Configuration page displays (see Figure 3-22).



Configuration :: Time

Time Configuration

Current sensor time Tuesday Jun 03 04:43:36 PM EDT 2003

Manual Time 04 : 43 PM Time Zone UTC Date 03 June 2003

Enable Automatic Time Configuration ☑

Time Zone CST6CDT

● Use Default NTP Servers View Default NTP Server List

○ Custom NTP Server(s)

Any changes to time require a reboot of the Sensor. Any NTP server changes that change the time on the Sensor by more than 1 second requires a reboot. Rebooting the Sensor will take the Sensor offline for approximately five minutes.

Changes to NTP servers or custom NTP server that do not affect the time more than 1 second can be applied and restarted.

Figure 3-22 Time Configuration Page

Step 2 To set the time manually, go to "Manual Time Configuration" on page 3-33
-OR-
To use an NTP server to set the time, go to "Automatic Time Configuration" on page 3-34.

Manual Time Configuration

Step 3 To set the time and date manually, click on the appropriate pull-down list (**Hour**, **Minute**, **AM/PM**, **Time Zone**, **Day**, **Month**, and **Year**) and select the value(s) as needed.

Note that the time zones are labeled with both a name and numerical value. The numerical value indicates the number of hours offset from UTC (Coordinated Universal Time), formerly called GMT (Greenwich Mean Time). The twelve time zones to the east of UTC are designated as "UTC +x hours" and the twelve time zones to the west of UTC are designated as "UTC -x hour". For example, in Figure 3-22 the CST6CDT is interpreted as "Central Standard Time -6 hours from UTC with Central Daylight (Saving) Time".

Step 4 Click on the **Apply & Reboot Sensor** button to reboot the Sensor to use the updated time/date.

Automatic Time Configuration

This procedure lets you add a new Network Time Protocol (NTP) server so that you can synchronize the Sensor's clock with it over the network. Use of this feature overrides any manual time settings that you may have made.

Step 1 To configure the Sensor to automatically synchronize with an NTP server, click on the **Enable Automatic Time Configuration** checkbox to select it.

The window refreshes with automatic time options displayed. The manual time configuration options are grayed and unavailable. (In Figure 3-22, the manual time configurations are shown ungrayed for illustration purposes.)

Step 2 To set the time zone, click on the **Time Zone** pull-down list and select the appropriate time zone for the Sensor's location.

Note that the time zones are labeled with both a name and numerical value. The numerical value indicates the number of hours offset from UTC (Coordinated Universal Time), formerly called GMT (Greenwich Mean Time). The twelve time zones to the east of UTC are designated as "UTC +x hours" and the twelve time zones to the west of UTC are designated as "UTC -x hour". For example, in Figure 3-22 the CST6CDT is interpreted as "Central Standard Time -6 hours from UTC with Central Daylight (Saving) Time".

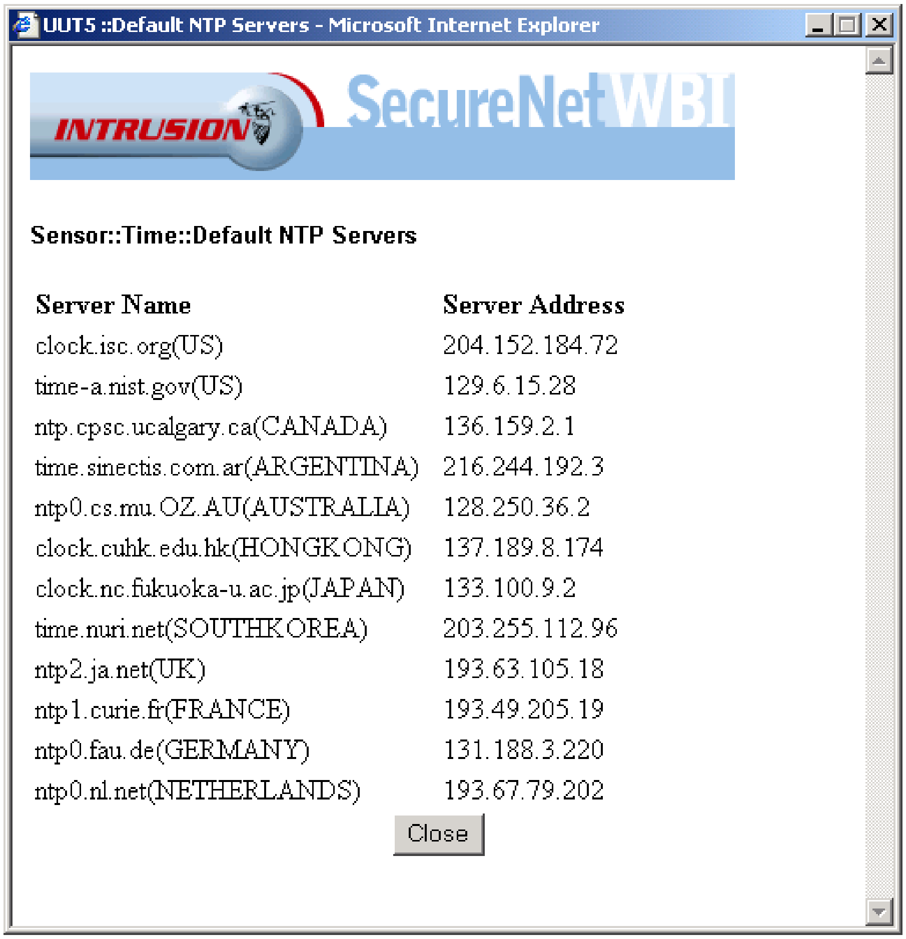
Step 3 If you want to synchronize the Sensor's clock to preselected default NTP servers, go to Step 4 in this procedure.
-OR-
If you want to synchronize the Sensor's clock to one or more specified NTP servers, go to Step 7 in this procedure.

Step 4 To synchronize to default NTP servers, click on the **Use Default NTP Servers** radio button to select it.

A View Default NTP Server List link displays.

Step 5 If you want to view a list of the default NTP servers, click on the **View Default NTP Server List** link.

The Default NTP Servers list displays in a new window (see Figure 3-23).



Sensor::Time::Default NTP Servers

Server Name	Server Address
clock.isc.org(US)	204.152.184.72
time-a.nist.gov(US)	129.6.15.28
ntp.cpsc.ucalgary.ca(CANADA)	136.159.2.1
time.sinectis.com.ar(ARGENTINA)	216.244.192.3
ntp0.cs.mu.OZ.AU(AUSTRALIA)	128.250.36.2
clock.cuhk.edu.hk(HONGKONG)	137.189.8.174
clock.nc.fukuoka-u.ac.jp(JAPAN)	133.100.9.2
time.nuri.net(SOUTHKOREA)	203.255.112.96
ntp2.ja.net(UK)	193.63.105.18
ntp1.curie.fr(FRANCE)	193.49.205.19
ntp0.fau.de(GERMANY)	131.188.3.220
ntp0.nl.net(NETHERLANDS)	193.67.79.202

Figure 3-23 Default NTP Servers List

Step 6 Close the Default NTP Servers list window (as needed) and then go to Step 11 on page 3-36.

Step 7 To synchronize to a specific NTP server, click on the **Custom NTP Server(s)** radio button to select it.

An Add a New NTP Server link displays.

Step 8 If you want to add an NTP server, click on the **Add a New NTP Server** link.

An empty text field displays.

Step 9 In the text field, type the IP address of the new NTP server in dotted-quad format.

You may add as many NTP servers as you like by repeating Step 8 and Step 9.

Step 10 If you want to delete an existing custom NTP server or you want to delete an empty custom ntp server field, click on the **Delete** link to the right of the field.

Step 11 Depending on the amount of time that your selections will change the Sensor's clock, click on the **Apply and Restart** button to apply the changes and restart the Sensor daemon
-OR-
click on the **Apply & Reboot Sensor** button to apply the changes and reboot the Sensor appliance.

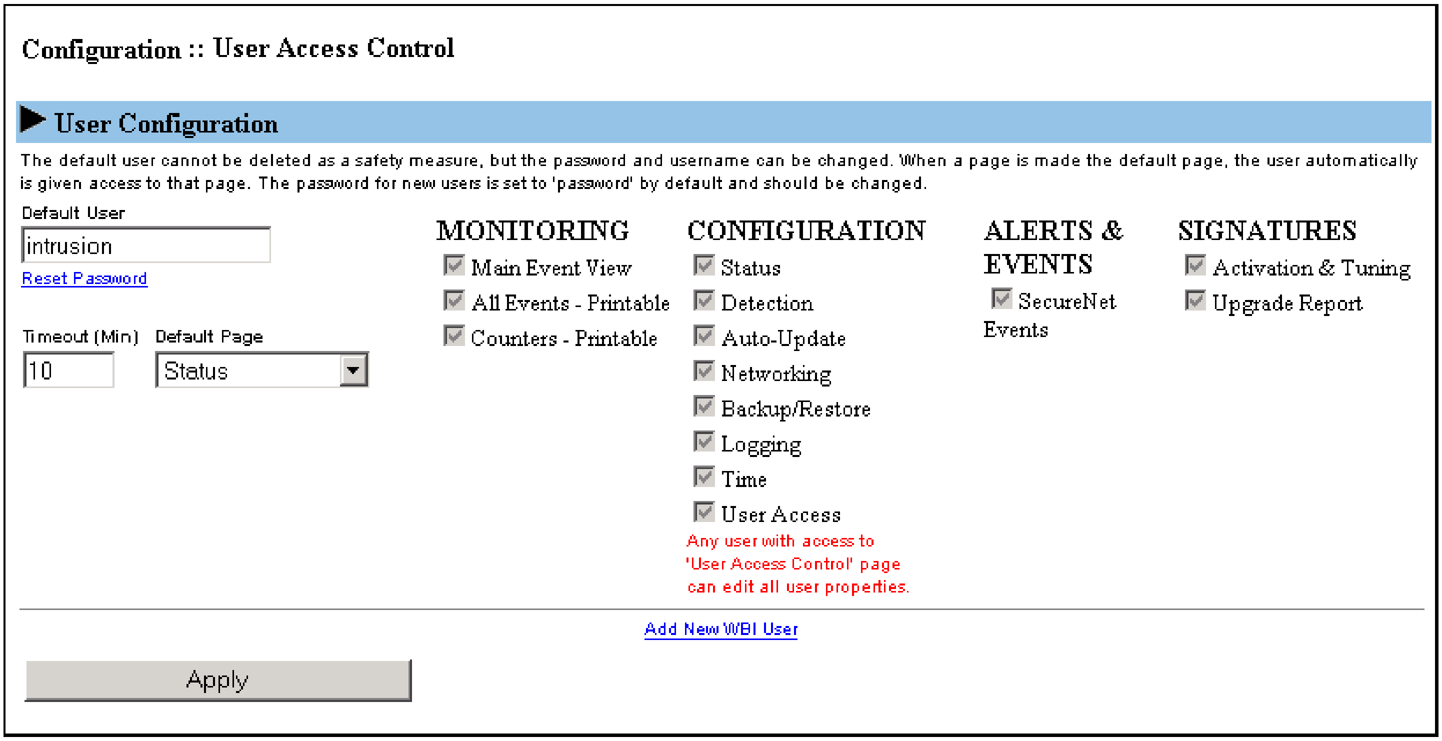
For any changes that do not affect the time at all or change the time by less than one second, you can click on **Apply and Restart**. If you mistakenly click on it, a warning message tells you that you must use the **Apply & Reboot Sensor** button instead.

Configure User Access Options

To configure User access to the SecureNet WBI, perform the following steps:

Step 1 At the top of any Intrusion SecureNet WBI page, click on the **Configuration** menu and then choose **User Access**.

The User Access Control Configuration page displays (see Figure 3-24).



Configuration :: User Access Control

▶ User Configuration

The default user cannot be deleted as a safety measure, but the password and username can be changed. When a page is made the default page, the user automatically is given access to that page. The password for new users is set to 'password' by default and should be changed.

Default User: intrusion

Reset Password

Timeout (Min): 10

Default Page: Status

MONITORING
- ☑ Main Event View
- ☑ All Events - Printable
- ☑ Counters - Printable

CONFIGURATION
- ☑ Status
- ☑ Detection
- ☑ Auto-Update
- ☑ Networking
- ☑ Backup/Restore
- ☑ Logging
- ☑ Time
- ☑ User Access

Any user with access to 'User Access Control' page can edit all user properties.

ALERTS & EVENTS
- ☑ SecureNet Events

SIGNATURES
- ☑ Activation & Tuning
- ☑ Upgrade Report

Add New WBI User

Figure 3-24 User Access Control Configuration Page

This page displays user profile information and it lets you make changes to it. In the case shown in Figure 3-24, the only user is the default user (initially set to "intrusion") and therefore has all available rights and privileges, including User Access Control (the ability to add, change, and delete user accounts). While the default user name can be changed, the default user's access rights and privileges cannot be changed.

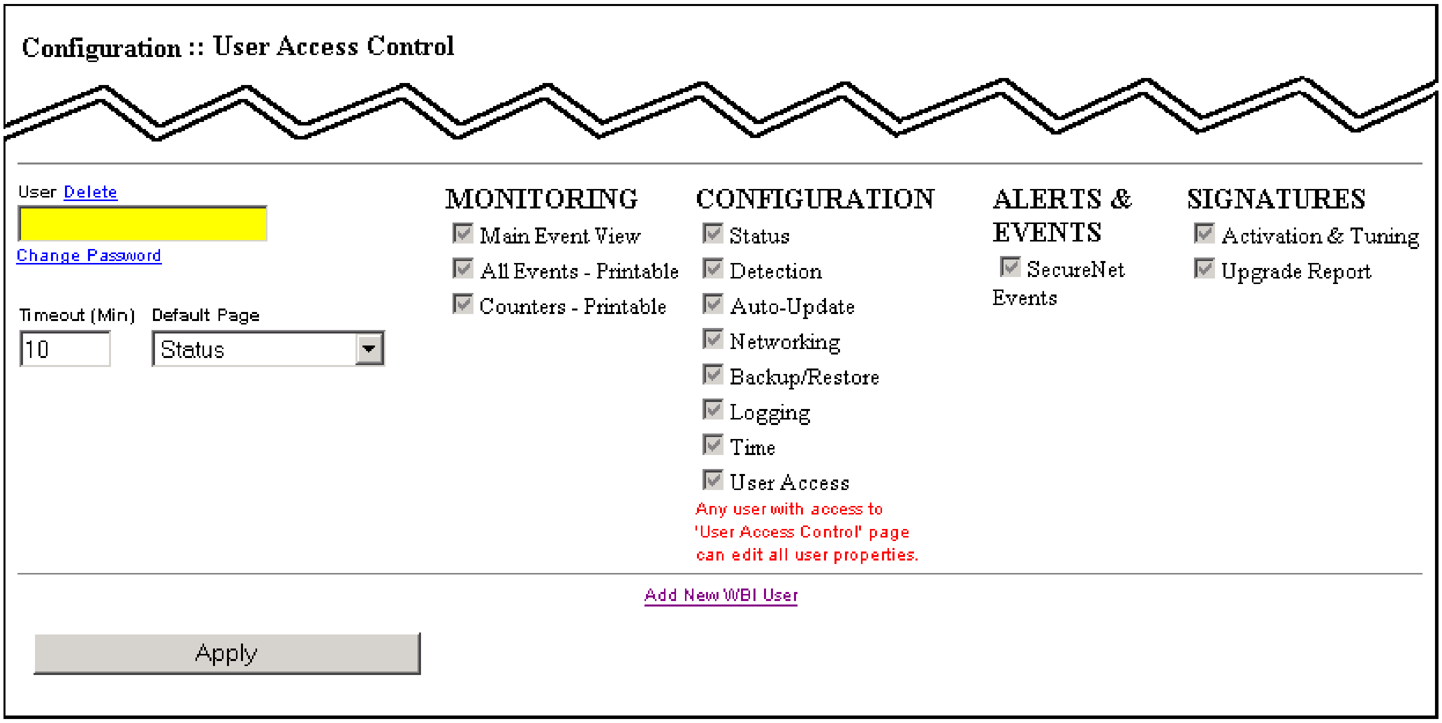
The default user's profile displays at the top of the User Configuration area. The User profiles for any users that are added will display below the default profile.

Step 2 To add a new user profile, go to "Add a New User" on page 3-37.
-OR-
To edit a user profile, go to "Edit a User Profile" on page 3-39.
-OR-
To delete a user profile, go to "Delete a User Profile" on page 3-41.

Add a New User

Step 1 On the User Access Control Configuration page, click on the **Add New User** link.

The page redisplays with a blank user profile form for entering new user information (see Figure 3-25).



Configuration :: User Access Control

User Delete

Change Password

Timeout (Min) 10

Default Page Status

MONITORING
☑ Main Event View
☑ All Events - Printable
☑ Counters - Printable

CONFIGURATION
☑ Status
☑ Detection
☑ Auto-Update
☑ Networking
☑ Backup/Restore
☑ Logging
☑ Time
☑ User Access

Any user with access to 'User Access Control' page can edit all user properties.

ALERTS & EVENTS
☑ SecureNet Events

SIGNATURES
☑ Activation & Tuning
☑ Upgrade Report

Figure 3-25 Add New User Form

By default, the Sensor Status page is accessible by all users and it is initially selected as the Default Page (the page that displays when the user logs in). The system idle Timeout value (the amount of time that the system can be idle before it automatically logs the user out) is set, to 10 minutes by default.

Step 2 In the **User** field, enter a unique user name.

The new User name may contain only upper-case and lower-case alphabetic characters (no numerals or special characters).

Step 3 If you want to change the idle Timeout, enter or edit the value (in minutes) in the **Timeout** field. The default value is 10 minutes.

Step 4 If you want to change the SecureNet WBI page that displays first when the user logs in, click on the **Default Page** field and select the page that you want from the pull-down list.

Any page that you select as the user's default page is automatically added to the list of pages to which the user has access.

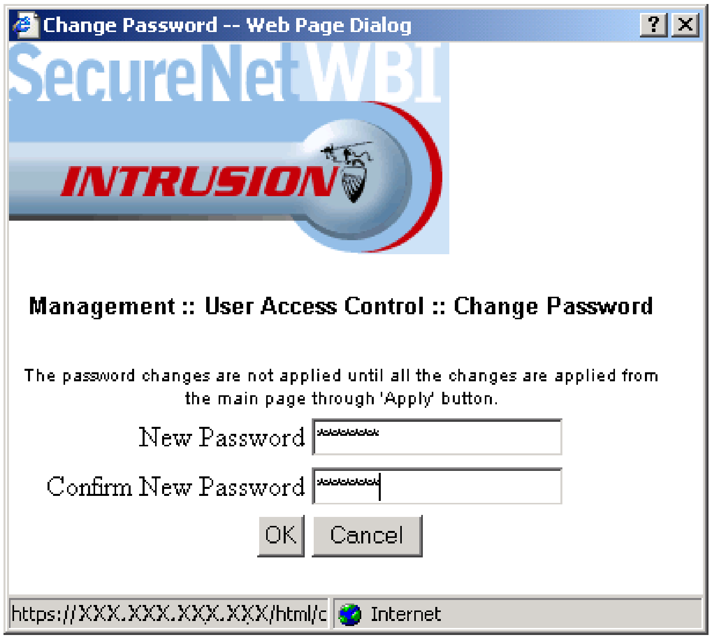
Step 5 Choose any additional pages to which the user is to have access by clicking on the checkboxes to select/deselect pages.

You cannot deselect the page that you have assigned as the user's default page. If you grant access to the User Access Control page, all pages are selected by default and you will not be able to deselect them.

Step 6 To change the user’s password:

a. Click on the **Change Password** link.

The Change Password Configuration page displays as a new window (see Figure 3-27).



Change Password -- Web Page Dialog

Management :: User Access Control :: Change Password

The password changes are not applied until all the changes are applied from the main page through 'Apply' button.

New Password ********

Confirm New Password ********

Figure 3-26 Change Password Configuration Page

b. In the **New Password** field, enter the new password.

The password should be at least 6 characters in length and can be constructed of any combination of alphanumeric and special characters.

c. In the **Confirm New Password** field, enter the new password again exactly as you entered it in the New Password field.

d. Click on the **OK** button.

The window closes and the password is changed.

Step 7 When you have completed making changes to the new User’s information, click on the **Apply** button to commit the changes.

The new user’s profile displays on the User Configuration below existing profiles. Additional users’ profiles display in the order in which they were created (they are not sorted for display).

Edit a User Profile

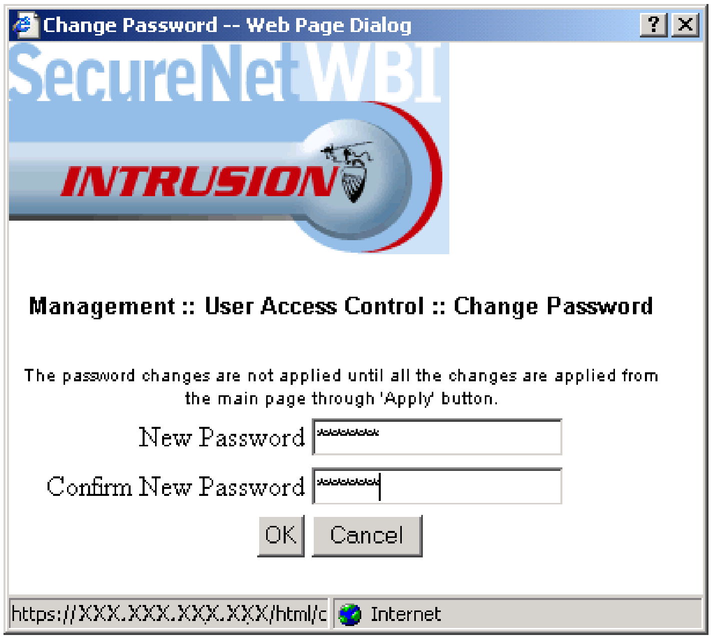
Step 1 On the User Access Control Configuration page, scroll as needed to display the user’s profile (see Figure 3-25).

Step 2 If you want to change the user’s login name, edit the existing name or select the existing name and then type a new name.

Step 3 If you want to change the user's password:

a. Click on the **Reset Password** link.

The Change Password Configuration page displays as a new window (see Figure 3-27).



Change Password -- Web Page Dialog

Management :: User Access Control :: Change Password

The password changes are not applied until all the changes are applied from the main page through 'Apply' button.

New Password: *******

Confirm New Password: *******

Figure 3-27 Change Password Configuration Page

b. In the **New Password** field, enter the new password.

The password should be at least 6 characters in length and can be constructed of any combination of alphanumeric and special characters.

c. In the **Confirm New Password** field, enter the new password again exactly as you entered it in the New Password field.

d. Click on the **OK** button.

The window closes. Go to Step 7 on page 3-41 to apply the new password. (If you do not apply the new password, it will not be changed.)

Step 4 If you want to change the idle timeout, enter or edit the value (in minutes) in the **Timeout** field. The default value is 10 minutes.

Step 5 If you want to change the SecureNet WBI page that displays first when the user logs in, click on the **Default Page** field and select the page that you want from the pull-down list.

Any page that you select as the user's default page is automatically added to the list of pages to which the user has access.

Step 6 Choose any additional pages to which the user is to have access by clicking on the checkboxes to select/deselect pages.

You cannot deselect the page that is assigned as the user's default page. If you grant access to the User Access Control page, all pages are selected by default and you will not be able to deselect them.

Step 7 When you have completed making changes to the User's information, click on the **Apply** button to commit the changes.

Delete a User Profile

Step 1 On the User Access Control Configuration page, scroll as needed to display the user's profile (see Figure 3-25).

Step 2 Click on the **Delete** link above the User Name field.

A confirmation dialog displays.

Step 3 Click on the **Yes** button.

The user's profile is deleted.

Step 4 Click on the **Apply** button to commit the changes.

Configure Alerts & Events Options

The Alerts & Events menu (see Figure 3-1) can be accessed from any Intrusion SecureNet WBI page.

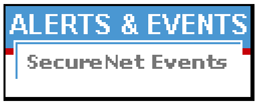


Figure 3-28 Alerts & Events Menu

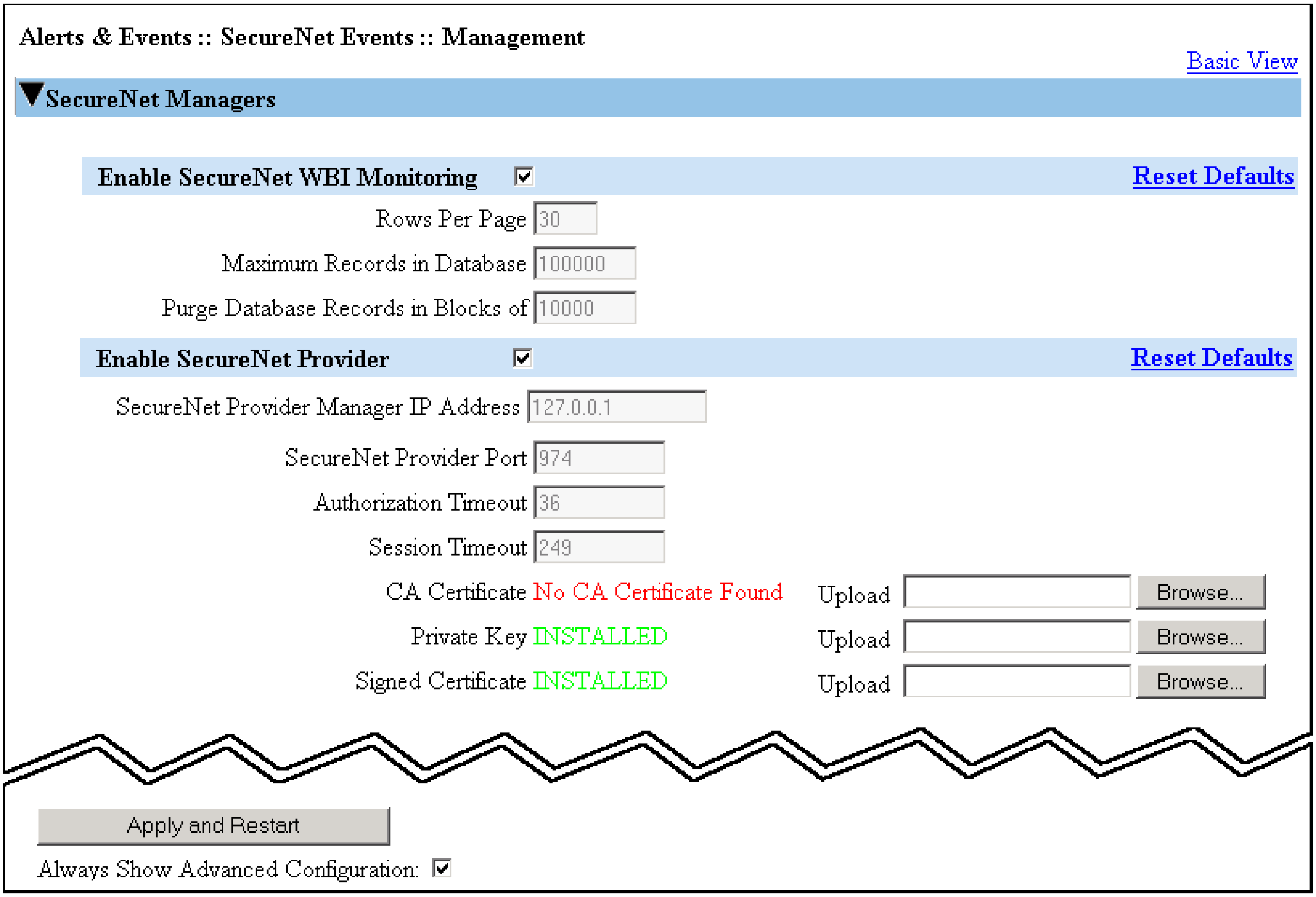
The following tasks can be performed:

- "Configure Intrusion SecureNet WBI Monitoring" on page 3-43
- "Configure SecureNet Provider" on page 3-44
- "Configure Email Alerting" on page 3-45
- "Configure SNMP Alerting" on page 3-46

To configure management, alerts, and events options, perform the following steps:

Step 1 At the top of any Intrusion SecureNet WBI page, click on the **Alerts & Events** menu and then choose **SecureNet Events**.

The Alerts & Events page displays as shown in Figure 3-29.



Alerts & Events :: SecureNet Events :: Management

Basic View

▼SecureNet Managers

Enable SecureNet WBI Monitoring ☑ Reset Defaults

Rows Per Page 30

Maximum Records in Database 100000

Purge Database Records in Blocks of 10000

Enable SecureNet Provider ☑ Reset Defaults

SecureNet Provider Manager IP Address 127.0.0.1

SecureNet Provider Port 974

Authorization Timeout 36

Session Timeout 249

CA Certificate No CA Certificate Found Upload [ ] Browse...

Private Key INSTALLED Upload [ ] Browse...

Signed Certificate INSTALLED Upload [ ] Browse...

Apply and Restart

Always Show Advanced Configuration: ☑

Figure 3-29 Alerts & Events Page (SecureNet Managers)

Note SecureNet SP-licensed users will not be able to make changes in the Enable WBI Monitoring area of the Configuration Page.

Configure Intrusion SecureNet WBI Monitoring

Step 2 To enable/disable the SecureNet Provider to monitor this Intrusion SecureNet WBI, click on the checkbox to the right of the **Enable SecureNet WBI Monitoring** subheader.

Step 3 In the **Rows Per Page** field, type or edit the number (1 to 999) to set the maximum number of table rows that you want to view on a GUI page. The default is 30.

Step 4 In the **Maximum Records Database** field, type or edit the number (1 to 1000000) to set the maximum number of records that you want to allow to be in the Database. The default is 100,000 (one hundred thousand).

Step 5 In the **Purge Database Records in Blocks of** field, type or edit the number (1 to 100000) to set the maximum number of records that you want to be purged on rotation. The default is 10,000 (ten thousand).

Configure SecureNet Provider

Step 6 To type or edit the IP address for the SecureNet Provider Manager, type the address in dotted quad format in the **SecureNet Provider Manager IP Address** field.

Step 7 To type or edit the SecureNet Provider Manager port number, type the port number in the **SecureNet Provider Port** field.

Step 8 To set the maximum amount of time (in minutes) for an authorization to complete, type the number of minutes in the **Authorization Timeout** field.

Step 9 To set the maximum amount of time (in minutes) for a session to be idle, type the number of minutes in the **Session Timeout** field.

The status (**INSTALLED** or **No <item> Found**) of the SecureNet Provider Manager's CA Certificate, Private Key, and Signed Certificate display in the lower center of the SecureNet Provider Manager area of the Configuration page. For the SecureNet Provider Manager to function, all three of the items must be installed.

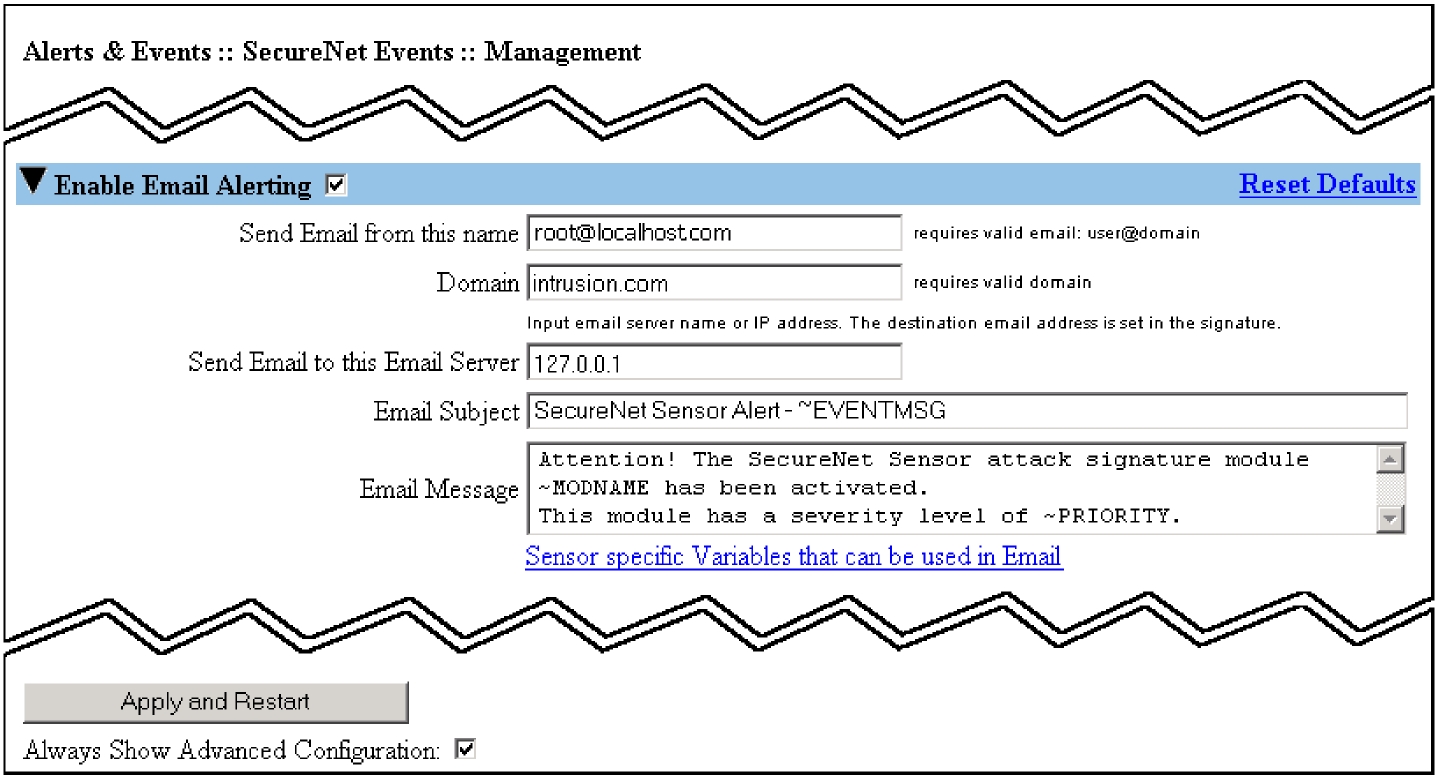
Step 10 To upload a new certificate or Private Key, type the complete path and name for the file to upload in the **Upload** text field
-OR-
Click on the **Browse** button and browse to the location of the file to upload.

Step 11 Click on the **Upload** button.

The specified certificate or Private Key uploads and the status for that item changes to **INSTALLED**.

Configure Email Alerting

Step 12 Scroll down the Alerts & Events page to display the Email Alerting area shown in Figure 3-30.



Alerts & Events :: SecureNet Events :: Management

▼ Enable Email Alerting ☑ Reset Defaults

Send Email from this name: root@localhost.com — requires valid email: user@domain

Domain: intrusion.com — requires valid domain

Input email server name or IP address. The destination email address is set in the signature.

Send Email to this Email Server: 127.0.0.1

Email Subject: SecureNet Sensor Alert - ~EVENTMSG

Email Message:

```
Attention! The SecureNet Sensor attack signature module
~MODNAME has been activated.
This module has a severity level of ~PRIORITY.
```

Sensor specific Variables that can be used in Email

Always Show Advanced Configuration: ☑

Figure 3-30 Alerts & Events Page (Email Alerting)

This area of the Alerts & Events page lets you set up an alert message to be sent to a designated email address upon the occurrence of an alert. It also lets you compose the subject and message text using Sensor-specific variables to insert text appropriate for the alert being reported.

Step 13 In the **Send Email from this name** field, type the "from" email address and then, in the **Domain** field, type the domain name.

In the example shown in Figure 3-30, the "from" email address is ***root@intrusion.com***.

Note You can display a list of the sensor-specific variables that can be used in the Email Subject and Email Message fields by clicking on the **Sensor specific Variables that can be used in Email Alert** link.

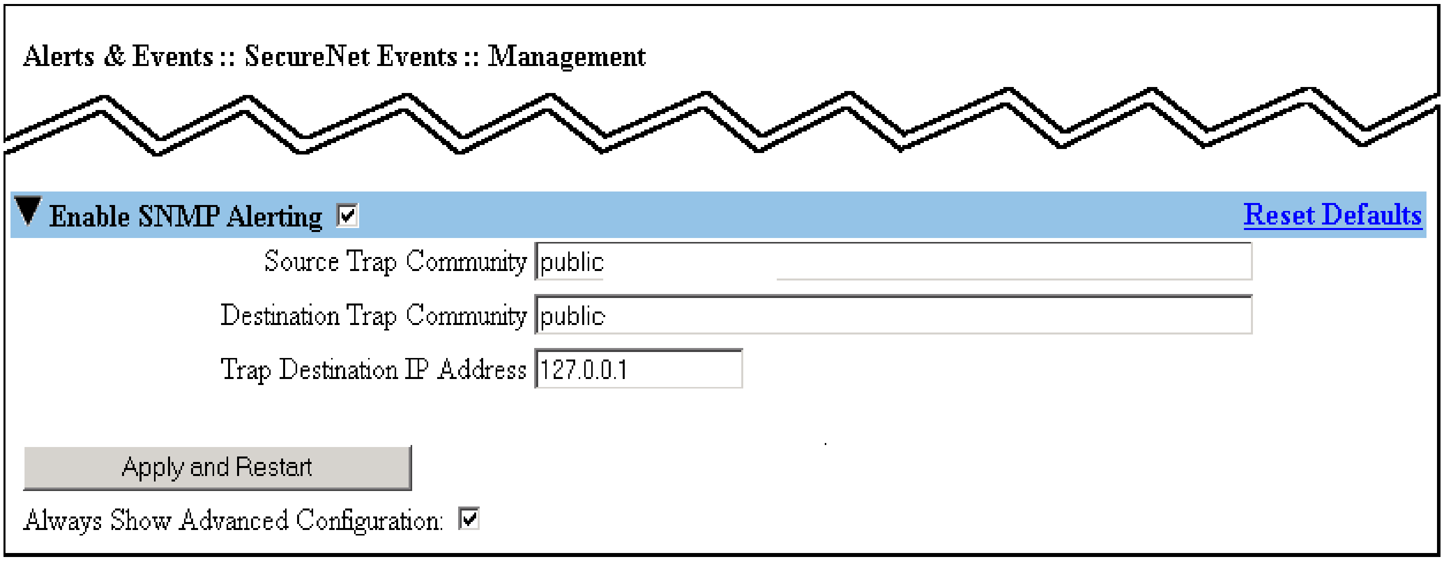
Step 14 In the **Email Subject** field, type or edit the subject of the email to be sent. You can include variables to insert text into the subject line of the email.

Step 15 In the **Email Message** field, type or edit the message (body) of the email to be sent. You can include variables to insert text into the message of the email.

Step 16 When you have finished making changes, click on the **Apply and Restart** button to apply your changes and restart the Sensor.

Configure SNMP Alerting

Step 17 Scroll down the page as needed to display the SNMP Alerting area as shown in Figure 3-31.



Alerts & Events :: SecureNet Events :: Management

▼ Enable SNMP Alerting ☑

Source Trap Community: public

Destination Trap Community: public

Trap Destination IP Address: 127.0.0.1

Always Show Advanced Configuration: ☑

Figure 3-31 Alerts & Events Page (Configure SNMP Alerting)

This area of the Alerts & Events page lets you enter the information needed to send SNMP traps to another device, usually Network Operations Center (NOC), for monitoring the status of individual network devices.

Step 18 To enable SNMP alerting, click on the **Enable SNMP Alerting** checkbox to select it.

Step 19 In the **Source Trap Community** field, type the Source Trap Community string that identifies the Sensor as the device sending SNMP traps.

Step 20 In the **Destination Trap Community** field, type the Destination Trap Community string that identifies the device that queries (or polls) the Sensor to send SNMP traps to itself.

Step 21 In the **Trap Destination IP Address** field, type the IP address that specifies the network location of the device that is receiving the SNMP traps.

Step 22 When you have finished making changes, click on the **Apply and Restart** button to apply your changes and restart the Sensor.

Configure Signatures Menu Options

The Signatures menu (see Figure 3-32) can be accessed from any Intrusion SecureNet WBI page.

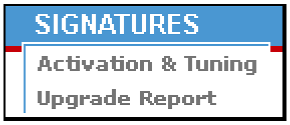


Figure 3-32 Signatures Menu

The following tasks can be performed:

- "Activate and Tune Signatures" on page 3-48
- "Display Signature Upgrade Report" on page 3-61

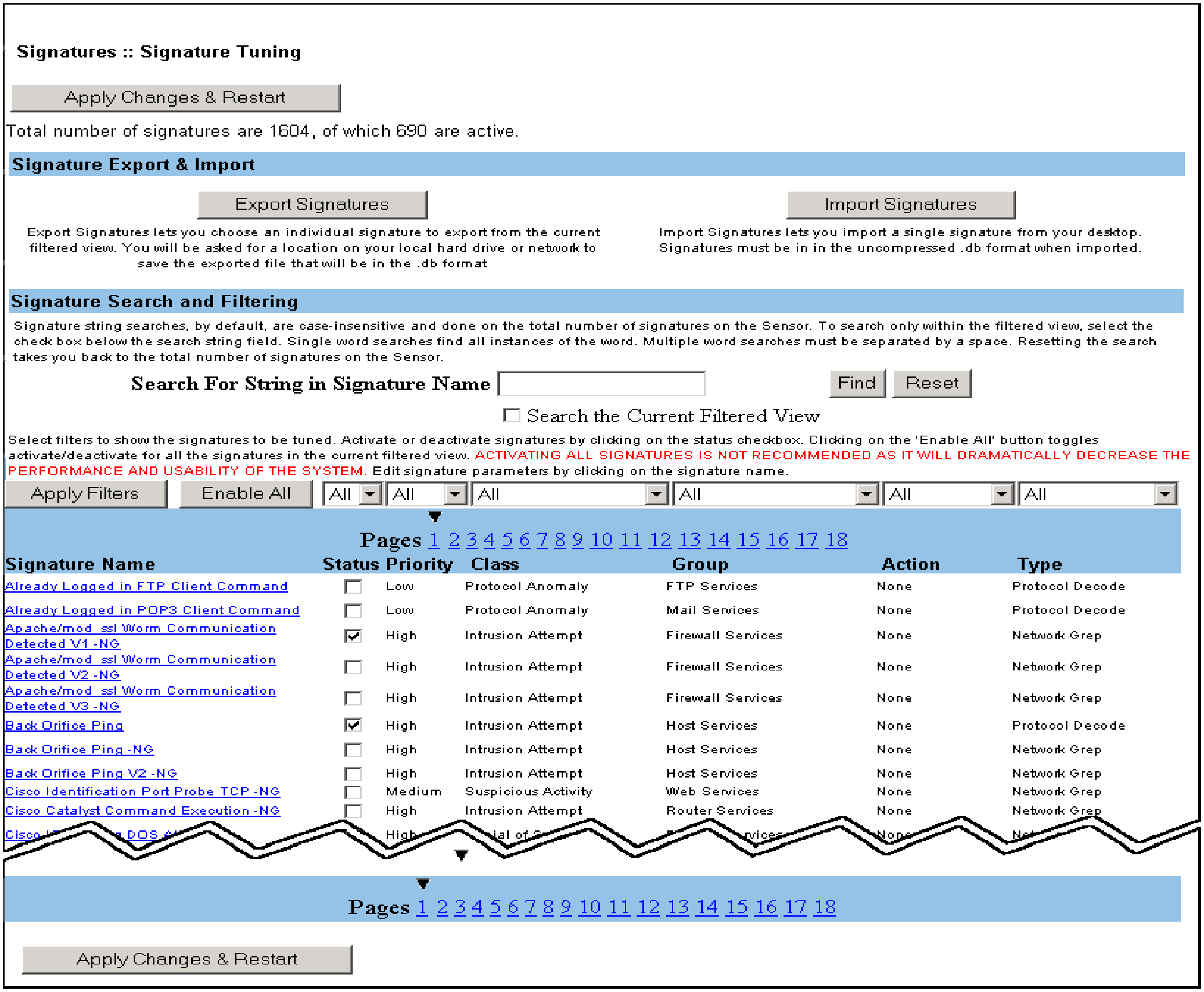
Activate and Tune Signatures

The Activation & Tuning page lets you perform the following tasks:

- "Export a Signature File" on page 3-49
- "Import a Signature File" on page 3-50
- "Search for Signatures by Text String" on page 3-51
- "View and Enable/Disable Signatures" on page 3-52

Step 1 At the top of any Intrusion SecureNet WBI page, click on the **Signatures** menu and then choose **Activation & Tuning**.

The Signature Tuning page displays (see Figure 3-33).



Signatures :: Signature Tuning

Apply Changes & Restart

Total number of signatures are 1604, of which 690 are active.

Signature Export & Import

Export Signatures

Export Signatures lets you choose an individual signature to export from the current filtered view. You will be asked for a location on your local hard drive or network to save the exported file that will be in the .db format

Import Signatures

Import Signatures lets you import a single signature from your desktop. Signatures must be in in the uncompressed .db format when imported.

Signature Search and Filtering

Signature string searches, by default, are case-insensitive and done on the total number of signatures on the Sensor. To search only within the filtered view, select the check box below the search string field. Single word searches find all instances of the word. Multiple word searches must be separated by a space. Resetting the search takes you back to the total number of signatures on the Sensor.

Search For String in Signature Name [ ] Find Reset

□ Search the Current Filtered View

Select filters to show the signatures to be tuned. Activate or deactivate signatures by clicking on the status checkbox. Clicking on the 'Enable All' button toggles activate/deactivate for all the signatures in the current filtered view. ACTIVATING ALL SIGNATURES IS NOT RECOMMENDED AS IT WILL DRAMATICALLY DECREASE THE PERFORMANCE AND USABILITY OF THE SYSTEM. Edit signature parameters by clicking on the signature name.

Apply Filters | Enable All | All | All | All | All | All | All

Pages 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

Signature Name	Status	Priority	Class	Group	Action	Type
Already Logged in FTP Client Command	□	Low	Protocol Anomaly	FTP Services	None	Protocol Decode
Already Logged in POP3 Client Command	□	Low	Protocol Anomaly	Mail Services	None	Protocol Decode
Apache/mod_ssl Worm Communication Detected V1 -NG	☑	High	Intrusion Attempt	Firewall Services	None	Network Grep
Apache/mod_ssl Worm Communication Detected V2 -NG	□	High	Intrusion Attempt	Firewall Services	None	Network Grep
Apache/mod_ssl Worm Communication Detected V3 -NG	□	High	Intrusion Attempt	Firewall Services	None	Network Grep
Back Orifice Ping	☑	High	Intrusion Attempt	Host Services	None	Protocol Decode
Back Orifice Ping -NG	□	High	Intrusion Attempt	Host Services	None	Network Grep
Back Orifice Ping V2 -NG	□	High	Intrusion Attempt	Host Services	None	Network Grep
Cisco Identification Port Probe TCP -NG	□	Medium	Suspicious Activity	Web Services	None	Network Grep
Cisco Catalyst Command Execution -NG	□	High	Intrusion Attempt	Router Services	None	Network Grep
Cisco DOS A		High	ial of S	vices	None	Ne

Pages 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

Apply Changes & Restart

Figure 3-33 Signature Tuning Page

The Activation & Tuning page displays installed signatures in alphabetic order for ease of reference. From this page you can view a list of all installed signatures, apply a display filter to view only signatures with certain characteristics, and enable or disable signatures individually or in groups.

Note SecureNet SME-licensed users will see only high-priority signatures on the Signature Tuning page. SecureNet SP-licensed users cannot access the Signature Tuning page.

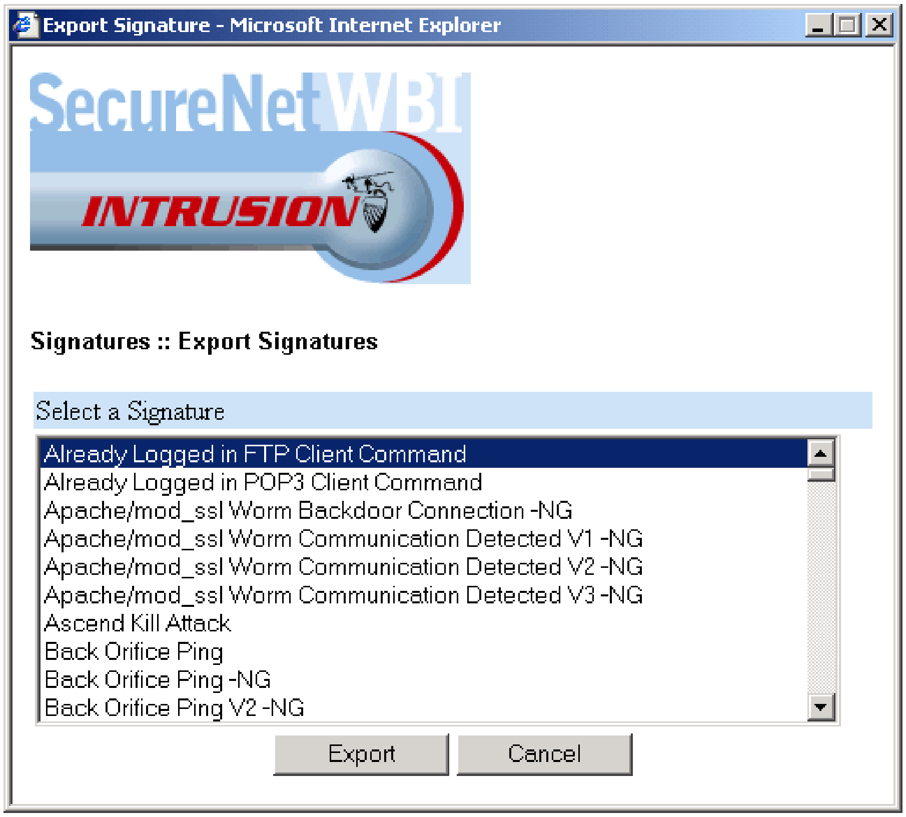
In the example shown in Figure 3-33, there is a total of 1604 signatures currently on the Sensor (690 of which are currently activated) presented on eighteen pages. You can navigate to any page by clicking on the page number in the **Pages** links at the top and bottom of every page.

Export a Signature File

Network grep signatures are stored as individual files in the Sensor's database and can be downloaded from the Sensor to your local workstation. To export a network grep signature file from the Sensor to a location on your workstation, perform the following steps:

Step 1 On the Signature Tuning page (see Figure 3-33), click on the **Export Signatures** button.

The Export Signature dialog displays the signatures in the current filtered view in a new window (see Figure 3-34).



Signatures :: Export Signatures

Select a Signature

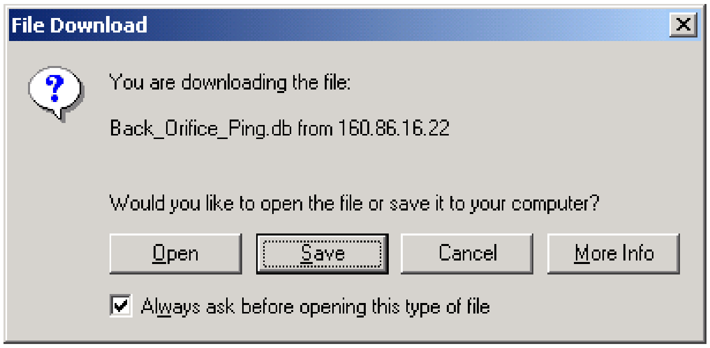
Already Logged in FTP Client Command
Already Logged in POP3 Client Command
Apache/mod_ssl Worm Backdoor Connection -NG
Apache/mod_ssl Worm Communication Detected V1 -NG
Apache/mod_ssl Worm Communication Detected V2 -NG
Apache/mod_ssl Worm Communication Detected V3 -NG
Ascend Kill Attack
Back Orifice Ping
Back Orifice Ping -NG
Back Orifice Ping V2 -NG

Figure 3-34 Export Signature Dialog

Step 2 Scroll as needed through the **Select a Signature** list and select the signature that you want to export.

Step 3 Click on the **Export** button.

A File Download dialog displays (see Figure 3-35).



File Download

You are downloading the file:

Back_Orifice_Ping.db from 160.86.16.22

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

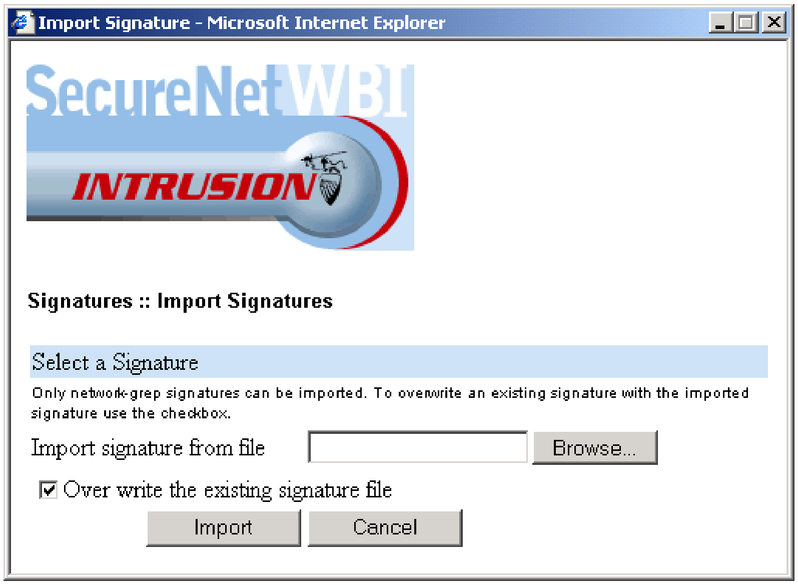
Figure 3-35 Export File Download Dialog

Import a Signature File

Network grep signatures are available as individual files that can be downloaded from the Intrusion website http://www.intrusion.com/products/signature.aspx to your local workstation. To import a network grep signature file from your workstation into the Sensor, perform the following steps:

Step 1 On the Signature Tuning page (see Figure 3-33), click on the **Import Signatures** button.

The Import Signatures dialog displays in a new window (see Figure 3-36).



Import Signature - Microsoft Internet Explorer

Signatures :: Import Signatures

Select a Signature

Only network-grep signatures can be imported. To overwrite an existing signature with the imported signature use the checkbox.

Import signature from file

☑ Over write the existing signature file

Figure 3-36 Import Signature Dialog

Step 2 If you want the imported signature file to overwrite an existing signature file with the same name, click on the **Overwrite the existing signature file** checkbox as needed to *select* it.
-OR-
If you want to save the imported signature file using a different filename, click on the **Overwrite the existing signature file** checkbox as needed to *deselect* it.

Step 3 In the **Import Signatures from file** text box, type the complete path and filename of the signature file to be imported.
-OR-
Click on the **Browse** button and then browse to the location of the signature file to be imported.

Step 4 Click on the **Import** button.

The specified file is imported. If a file with the same name as the imported file does not exist or a file with that name exists but you chose to have the existing file with the same name overwritten, the file is saved using its original name.
-OR-
If you chose not to overwrite the existing file, an error dialog displays indicating that the specified file cannot be imported because you chose to not overwrite the existing file.

Search for Signatures by Text String

Step 5 To search the Sensor's database for signatures based on strings contained in the signature name, perform the following steps:

a. If you want to search only the current filtered list of signatures, click on the **Search the Current Filtered View** checkbox to select it; if you want to search the entire list of installed signatures, leave the checkbox deselected.

b. In the **Search for String in Signature Name** field, type the exact string that you want to search for and then click on the **Find** button.

   The current view displays the results from the string search you specified.

View and Enable/Disable Signatures

Step 6 To view and enable/disable signatures, perform the following steps:

a. Click on the appropriate number in the **Pages** field to navigate through the alphabetized list of signatures.

b. Click on the pull-down menus on the top of the signature list to select from the following options for filtering the display of signatures:

Status	All, On, or Off
Priority	All, High, Medium, or Low
Class	All, Intrusion Attempt, Denial of Service, Distributed DoS, Suspicious Activity, Protocol Anomaly, or Network Event
Group	All, Firewall, FTP, Host, IDS, Instant Messaging, Mail, Network Information, News, Remote Access, Router, or Web
Action	All, None, Text Log, TCP Dump, or Binary Log
Type	All, Protocol Decode, or Network Grep

c. When you are finished making filtering choices, click on the **Apply Filters** button to display only the signatures that match your filtering selections.

Important! Enabling all signatures will dramatically reduce the performance and usability of your Sensor and is NOT recommended.

d. Click on the **Status** checkbox to enable or disable signatures
-OR-
Click on the **Enable All** button to activate or deactivate all of the signatures (that is, to check or uncheck the Status checkboxes for all the signatures). If you choose to **Enable All**, you should go through the list of signatures and uncheck the Status checkbox for those signatures that you do not want to use. If you choose to **Disable All**, you should go through the list and check the Status checkbox for those signatures that you do want to use.

e. If you changed the status of signatures in the list, click on the **Apply and Restart** button to apply your changes and restart the Sensor.

Edit a Signature

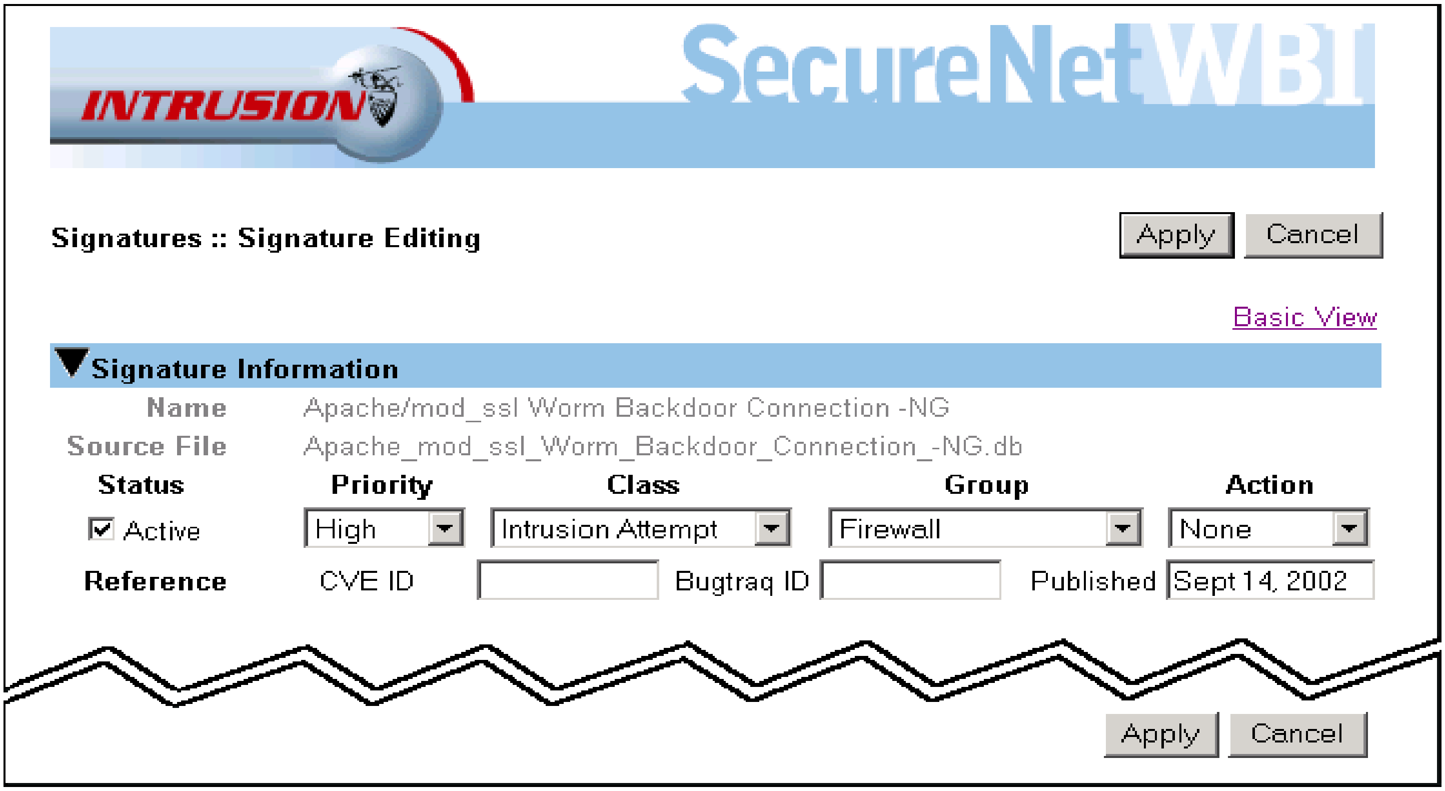
Note Only network grep signatures can be edited. Protocol decode signatures cannot be edited.

To edit a signature in the Sensor database, perform the following steps:

Step 1 On the Signature Tuning page (see Figure 3-33), click on the **Import Signatures** button.

Step 1 Click on the signature name to be edited.

The Signature Editing page for that signature displays in a new window (see Figure 3-37).



Signatures :: Signature Editing

▼ Signature Information

Name	Apache/mod_ssl Worm Backdoor Connection -NG
Source File	Apache_mod_ssl_Worm_Backdoor_Connection_-NG.db

Status	Priority	Class	Group	Action
☑ Active	High	Intrusion Attempt	Firewall	None

Reference CVE ID Bugtraq ID Published Sept 14, 2002

Figure 3-37 Signature Editing Page (Signature Information)

The signature name and source file display in the Signature Information area. Signature Information on the Signature Editing page is dynamic; fields that apply and are editable are displayed in regular type. Use the pull-down menu fields and text fields to specify information, then scroll down to click the **Apply and Restart** button to apply your changes and restart the Sensor.

Step 2 To set the priority for a signature, click the **Priority** pull-down menu and choose **Low**, **Medium**, or **High**.

Step 3 To set the class for a signature, click the **Class** pull-down menu to set one of the following classes for a signature: **Intrusion Attempt**, **Denial of Service**, **Distributed DoS**, **Suspicious Activity**, **Protocol Anomaly**, or **Network Event**.

Step 4 To set a classification group for a signature, click the **Group** pull-down menu and choose one of the following groups: **Firewall**, **FTP**, **Host**, **IDS**, **Instant Messaging**, **Mail**, **Remote Access**, **Router**, or **Web**.

Step 5 To choose the action that should occur when the signature activates, click the **Action** pull-down menu and choose from the following actions: **None**, **Text Log**, **TCP Dump**, **TCP Reset**, or **Binary Log**.

Note The TCP Reset action can be used only when the Input Source is TCP Any, TCP Stream, or Null. The Text Log, TCP Dump, and Binary Log actions can be used only if content logging is enabled.

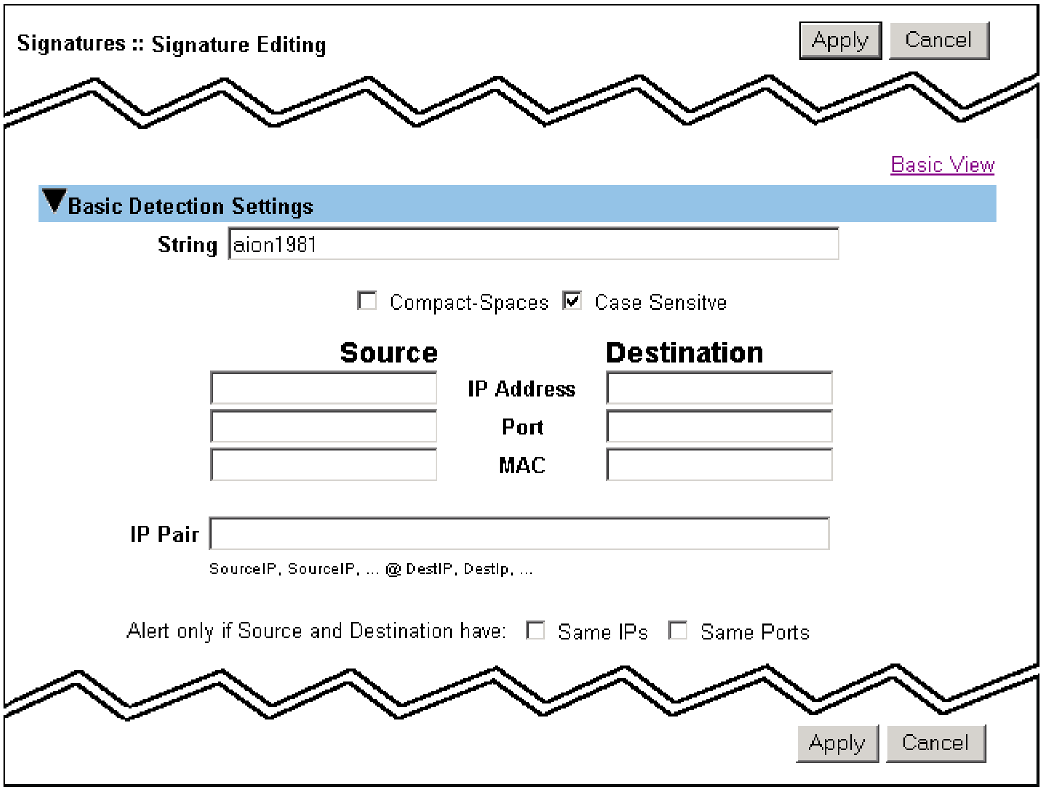
Step 6 To use the optional **Reference** fields to specify standard vulnerability information, specify CVE (Common Vulnerabilities and Exposures) or Bugtraq information as follows:

- In the **CVE ID** field, type the unique ID assigned to a vulnerability by the CVE Editorial Board and maintained by the MITRE Corporation. For more information, go to http://cve.mitre.org/
- In the **Bugtraq ID** field, type the unique ID number assigned to a vulnerability by Symantec and maintained in the Symantec SecurityFocus Bugtraq database. For more information, go to http://online securityfocus.com/
- In the **Published** field, type the earliest date that the vulnerability was published. (This date can be obtained from a Bugtraq entry, a CVE entry, a CERT advisory, a vendor advisory, and so forth.)

Step 7 When you are finished making changes, click on the **Apply** button at the top or bottom of the page.

Specify Basic Detection Settings

The Basic Detection Settings area of the Signature Editing page (see Figure 3-38) lets you specify details that affect the basic detection performed by signatures.



Signatures :: Signature Editing

Basic Detection Settings

String: aion1981

□ Compact-Spaces ☑ Case Sensitve

Source / Destination: IP Address, Port, MAC

IP Pair

SourceIP, SourceIP, ... @ DestIP, DestIp, ...

Alert only if Source and Destination have: □ Same IPs □ Same Ports

Figure 3-38 Signature Editing Page (Basic Detection Settings)

Step 8 To specify a network grep data scanning string for which the signature will have the Sensor search, type the characters to search for in the **String** field:

Note Specification of a network grep data scanning string is not supported with the Null input source type.

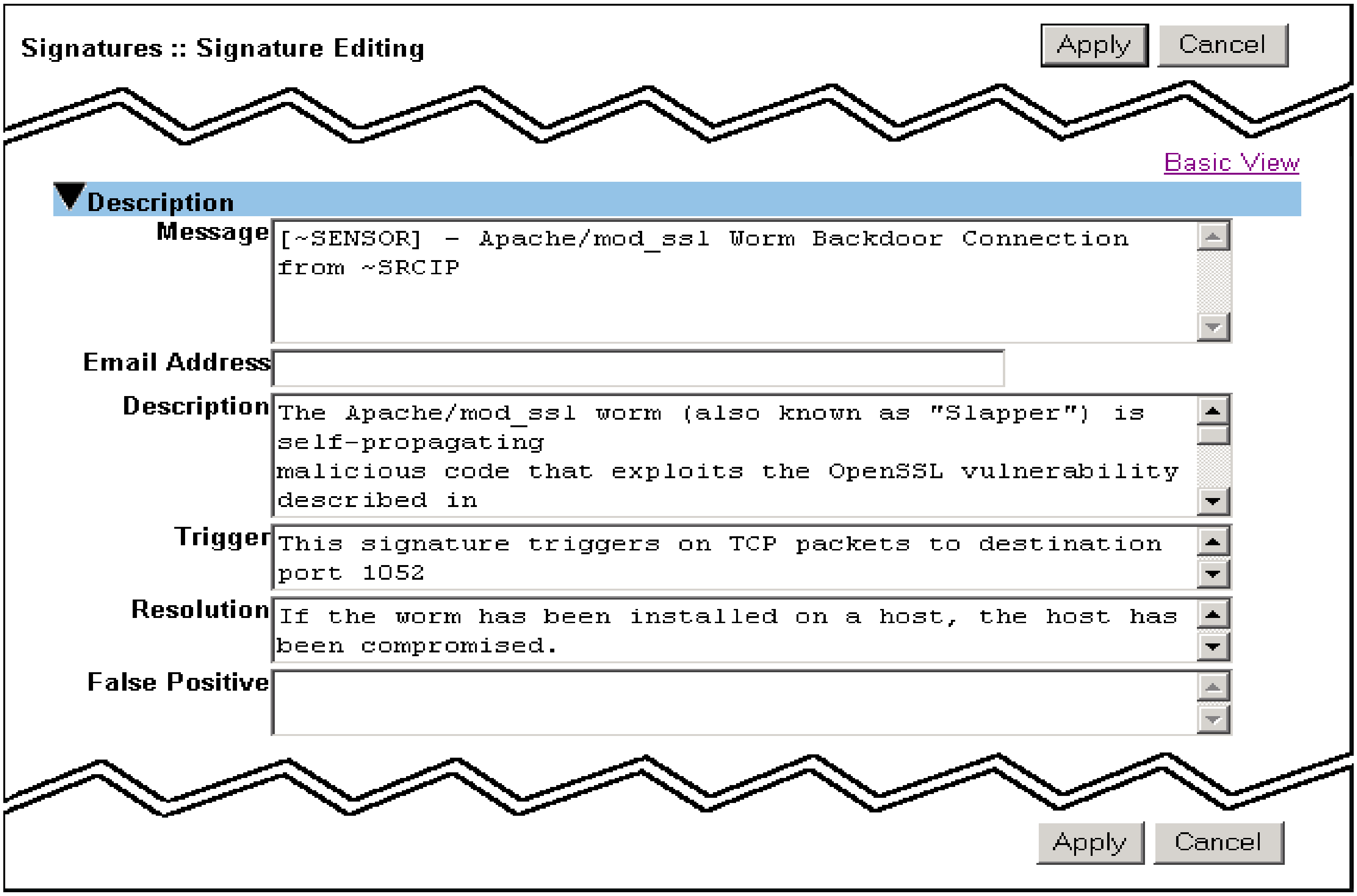
Use the two checkboxes after the **String** field (shown in Figure 3-38) if you need special handling of spaces between grep arguments or to specify case sensitivity for the network grep data scanning string.

- To compress white space (such as tabs and spaces) between extracted grep arguments into a single character, click on the **Compact-Spaces** checkbox.
- To have case to be considered when the search for network grep strings is performed, click on the **Case Sensitive** checkbox.

Step 9 When you are finished making changes, click on the **Apply** button at the top or bottom of the page.

View and Edit Signature Descriptions

Use the Description area of the Signature Editing page (see Figure 3-39) to view and edit description fields for a signature:



Message: [~SENSOR] - Apache/mod_ssl Worm Backdoor Connection from ~SRCIP

Email Address:

Description: The Apache/mod_ssl worm (also known as "Slapper") is self-propagating malicious code that exploits the OpenSSL vulnerability described in

Trigger: This signature triggers on TCP packets to destination port 1052

Resolution: If the worm has been installed on a host, the host has been compromised.

False Positive:

Figure 3-39 Signature Editing Page (Description)

Step 10 If you want to enable support for logging events in the database, type the log message in the **Message** field. Be sure to include any variables required to insert appropriate text to the message. Variables include:

- **~SENSOR** inserts the name of the affected Sensor into the message.
- **~ARGDATA0** inserts argument data into the message.
- **~SRCIP** inserts the source IP address into the message.
- **~DSTIP** inserts the destination IP address into the message.

Step 11 If you want to send an e-mail notification when the signature triggers, type in the **Email Address** field the e-mail address to which you want the message sent**.** The format of this parameter is *user@host.*

Note The **Email Address** option is configurable only if email notification is globally configured on the Sensor host and a log message (along with any required variables) has been specified in the **Message** field.

Step 12 Type a detailed description of the signature in the **Description** field.

Step 13 Type a description of what triggers the signature in the **Trigger** field.

Step 14 Type a description of what the user should do to mitigate the effects of the attack identified by the signature in the **Resolution** field.

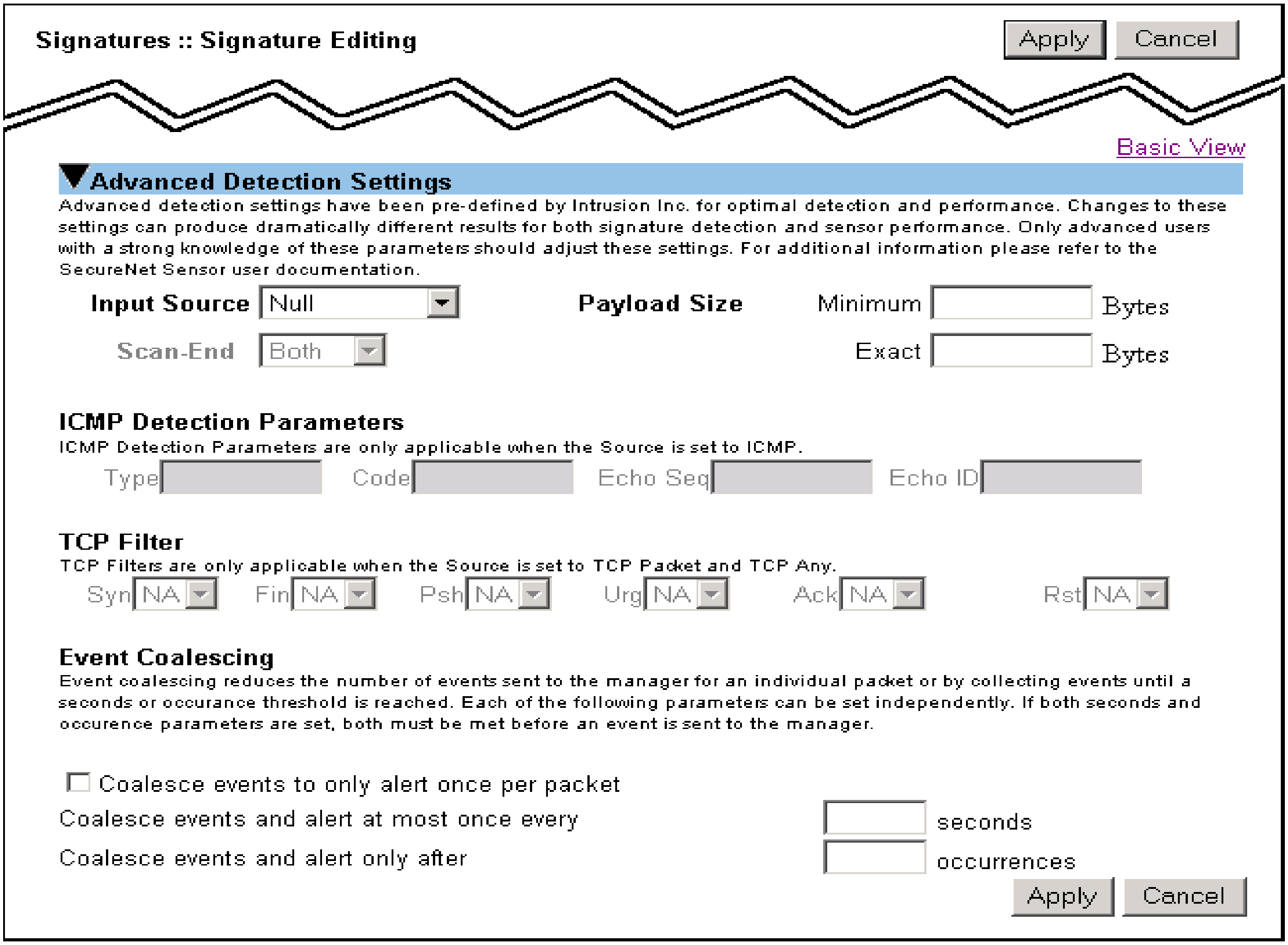
Step 15 Type a description of what constitutes a false positive of the attack defined by this signature in the **False Positive** field.

Step 16 After editing fields on the Signature Editing page, scroll down to the bottom of the page and click on the **Apply and Restart** to apply your changes and restart the Sensor.

Step 17 When you are finished making changes, click on the **Apply** button at the top or bottom of the page.

Configuring Advanced Detection for Signatures

The parameters for the Advanced Detection Settings display in the Advanced View only. Advanced users can use the Advanced Detection area of the Signature Editing page (see Figure 3-40) to specify the detection parameters.



Signatures :: Signature Editing

▼Advanced Detection Settings

Advanced detection settings have been pre-defined by Intrusion Inc. for optimal detection and performance. Changes to these settings can produce dramatically different results for both signature detection and sensor performance. Only advanced users with a strong knowledge of these parameters should adjust these settings. For additional information please refer to the SecureNet Sensor user documentation.

Input Source: Null

Scan-End: Both

Payload Size: Minimum ____ Bytes; Exact ____ Bytes

ICMP Detection Parameters

ICMP Detection Parameters are only applicable when the Source is set to ICMP.

Type ____ Code ____ Echo Seq ____ Echo ID ____

TCP Filter

TCP Filters are only applicable when the Source is set to TCP Packet and TCP Any.

Syn: NA Fin: NA Psh: NA Urg: NA Ack: NA Rst: NA

Event Coalescing

Event coalescing reduces the number of events sent to the manager for an individual packet or by collecting events until a seconds or occurance threshold is reached. Each of the following parameters can be set independently. If both seconds and occurence parameters are set, both must be met before an event is sent to the manager.

□ Coalesce events to only alert once per packet

Coalesce events and alert at most once every ____ seconds

Coalesce events and alert only after ____ occurrences

Figure 3-40 Signature Editing Page (Advanced Detection Settings)

Step 18 From the **Input Source** pull-down list, select an appropriate source of the type of network traffic examined by the module. The choices are **TCP Stream**, **TCP Packet**, **UDP Packet**, **ICMP Packet**, **IP Packet**, **Ether Packet**, **Raw Packet**, **Null**, **IGMP**, **IP Fragment**, **TCP Any**, and **HTTP**.

Step 19 To check for a payload of a certain size, specify information in the appropriate **Payload Size** fields.

- To look for a payload of at least a certain size, type the number of bytes in the **Minimum** field.
- To look for a payload of an exact size, type the number of bytes in the **Exact** field.

Note Payload size options are valid for SecureNet Sensor version 4.4 and newer.

Step 20 To indicate the end of a TCP connection circuit that should be scanned for a network grep string, make a selection using the **Scan-End** pull-down list. Choose **Client**, **Server**, or **Both**. The Scan-End option requires the specification of a value in the **String** field of the Signature Editing page.

Step 21 Specify **ICMP Detection Parameters** when the Input Source is ICMP. Specify the following options as required:

Type Type a number in the range 0-32767 to designate the type of ICMP message on which you want to filter (for examples, go to http://www.iana.org/assignments/icmp-parameters).

Code If the type of ICMP message has a code further identifying its function, type a number in the range 0-15 to designate the code on which you want to filter.

Echo Seq If the ICMP Type is 0 and the ICMP Code is 0, type a number between 0-16383 to indicate the sequence number on which you want to filter. Echo request packets contain a sequence number (starting at 0) which is incremented after each transmission

Echo ID If the ICMP Type is 0 and the ICMP Code is 0, type a number between 0-16383 to indicate the numeric value of the Echo ID on which you want to filter.

ICMP options are supported with SecureNet Sensor versions 4.4 and newer.

Step 22 Specify **TCP Filter** options when the Input Source type is TCP Packet.TCP filter fields specify how to filter based on the setting of TCP flags. Each field has a pull-down menu with three options: **No** (must not be present), **NA** (not applicable), and **Yes** (must be present). The default setting for each field is **NA**. Set the fields to Yes, No, or NA for TCP flags that operate as follows:

Syn Sets the TCP flag SYN for synchronizing/starting a packet from a source host

Fin Sets the TCP flag FIN for indicating that the source host has finished sending data.

Psh Sets the TCP flag PSH to push/pass the data to the application as soon as possible.

Urg Sets the TCP flag URG to indicate if the urgent pointer is valid.

Ack Sets the TCP flag ACK (acknowledgement flag).

Rst Sets the TCP flag RST (reset flag)

TCP filter options are valid with Sensor version 4.4 and later.

Step 23 To indicate the frequency of triggering for a signature, use the **Event Coalescing** fields. Click on the checkboxes to indicate whether a signature can be triggered more than once:

- **Coalesce Events to only alert once per packet**
- **Coalesce events and alert at most once every ____ seconds**: Type a value from 0-16383 to indicate the period (in seconds) that must elapse between alerts.
- **Coalesce events and alert only after ____ occurrences**: Type a value from 0-16383 to indicate the number of triggers that are allowed to occur before alerting or logging begins.

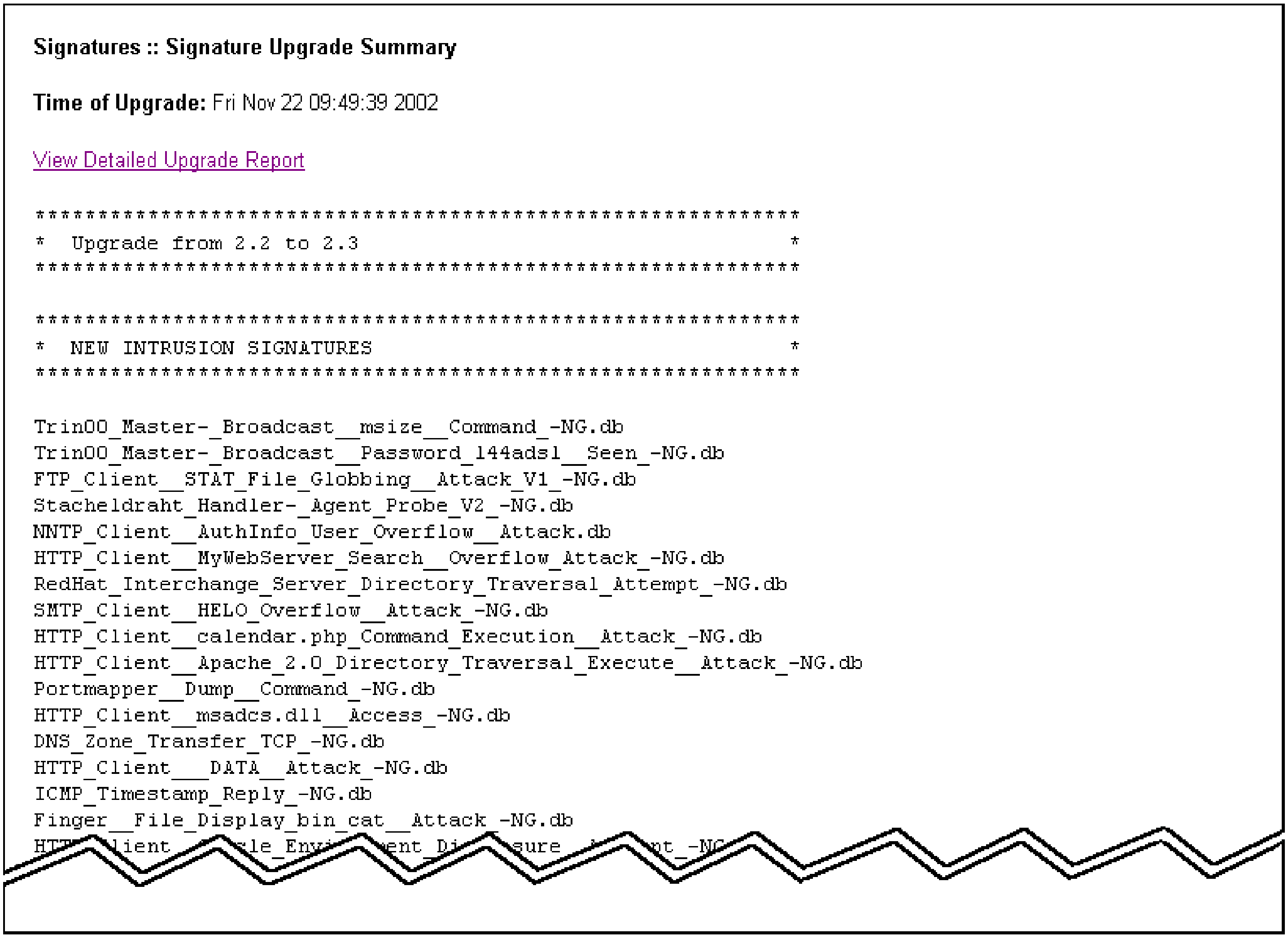
Each checkbox operates independently of the others. For example, you can have a signature trigger once every 300 seconds, but only after 3 occurrences.

Display Signature Upgrade Report

The Upgrade Report lets you view information about the changes that occurred during a signature pack upgrade.

Step 1 At the top of any Intrusion SecureNet WBI page, click on the **Signatures** menu and then choose **Upgrade Report**.

The Signature Upgrade Summary page displays (see Figure 3-41).



Signatures :: Signature Upgrade Summary

Time of Upgrade: Fri Nov 22 09:49:39 2002

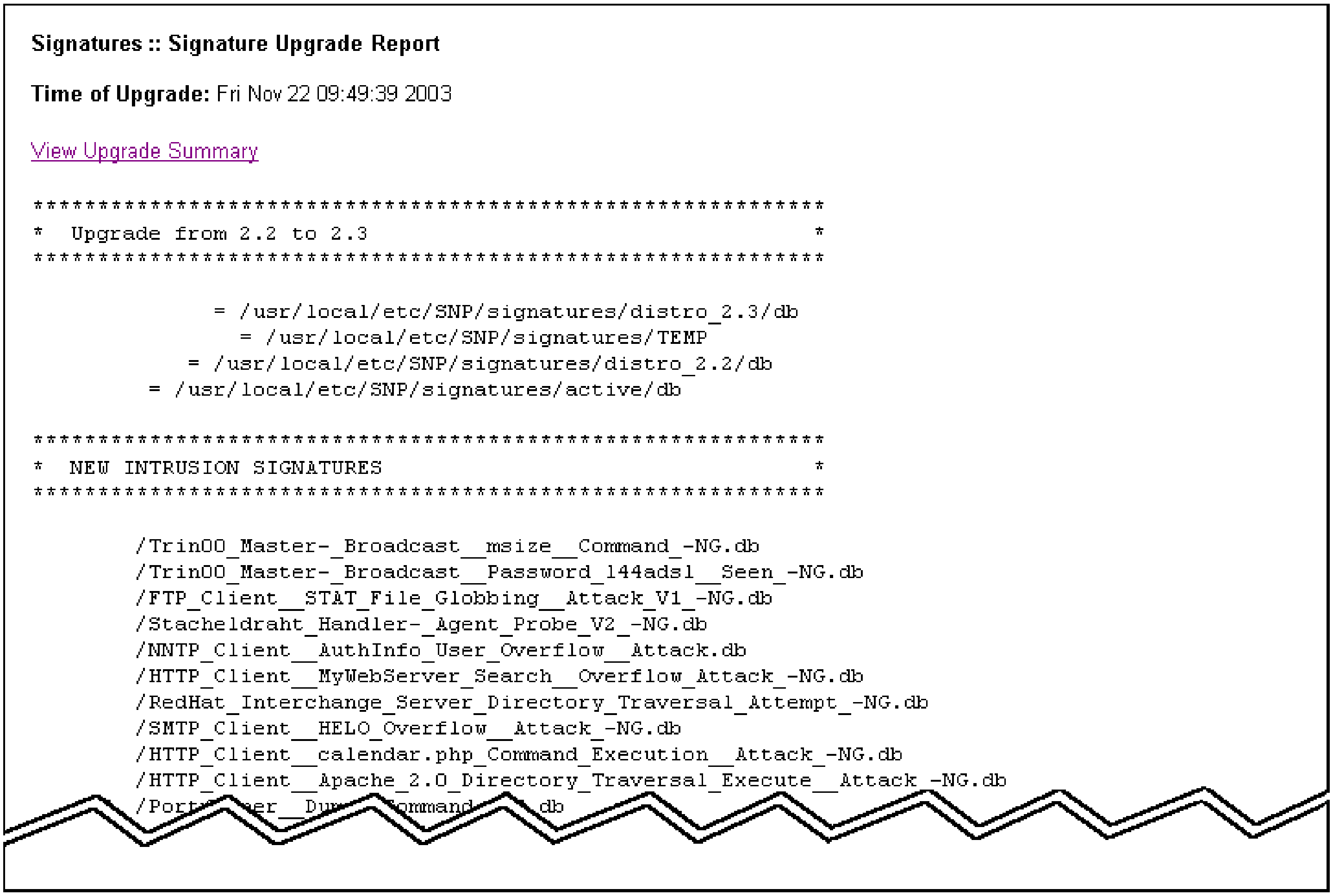
View Detailed Upgrade Report

```
************************************************************
*  Upgrade from 2.2 to 2.3                                  *
************************************************************

************************************************************
*  NEW INTRUSION SIGNATURES                                 *
************************************************************

Trin00_Master-_Broadcast__msize__Command_-NG.db
Trin00_Master-_Broadcast__Password_144adsl__Seen_-NG.db
FTP_Client__STAT_File_Globbing__Attack_V1_-NG.db
Stacheldraht_Handler-_Agent_Probe_V2_-NG.db
NNTP_Client__AuthInfo_User_Overflow__Attack.db
HTTP_Client__MyWebServer_Search__Overflow_Attack_-NG.db
RedHat_Interchange_Server_Directory_Traversal_Attempt_-NG.db
SMTP_Client__HELO_Overflow__Attack_-NG.db
HTTP_Client__calendar.php_Command_Execution__Attack_-NG.db
HTTP_Client__Apache_2.0_Directory_Traversal_Execute__Attack_-NG.db
Portmapper__Dump__Command_-NG.db
HTTP_Client__msadcs.dll__Access_-NG.db
DNS_Zone_Transfer_TCP_-NG.db
HTTP_Client___DATA__Attack_-NG.db
ICMP_Timestamp_Reply_-NG.db
Finger__File_Display_bin_cat__Attack_-NG.db
HTTP_Client__[illegible]le_Environment_Disclosure__[illegible]nt_-NG
```

Figure 3-41 Signature Upgrade Summary

The Signature Upgrade Summary page shows the time of the last upgrade, the old and new software versions, and a list of the new signatures installed with the upgrade.

Step 2 To list additional details about the upgrade, click on the **View Detailed Upgrade Report** link (see Figure 3-42).



Signatures :: Signature Upgrade Report

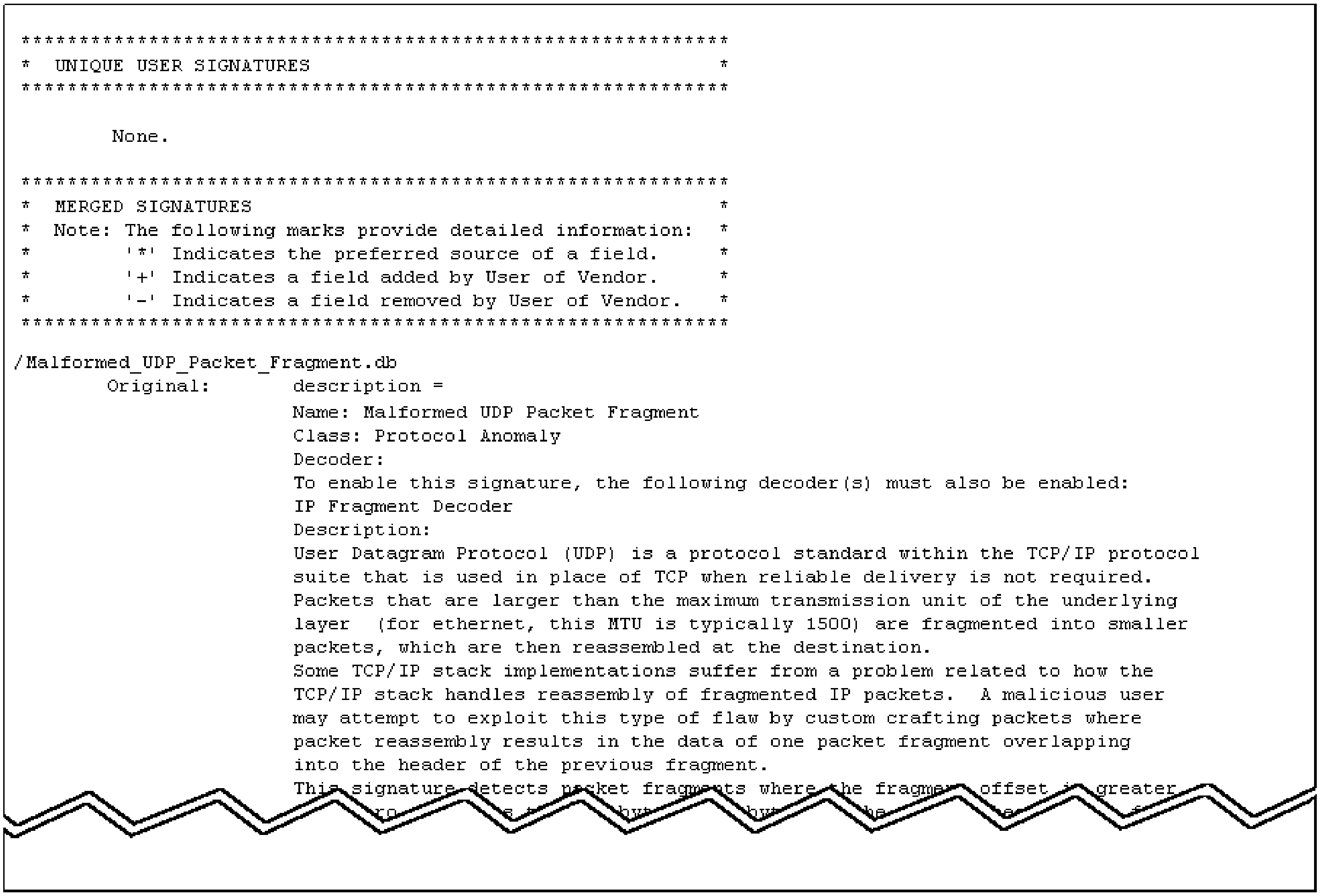
Time of Upgrade: Fri Nov 22 09:49:39 2003

View Upgrade Summary

```
*************************************************************
*  Upgrade from 2.2 to 2.3                                  *
*************************************************************

              = /usr/local/etc/SNP/signatures/distro_2.3/db
                = /usr/local/etc/SNP/signatures/TEMP
            = /usr/local/etc/SNP/signatures/distro_2.2/db
         = /usr/local/etc/SNP/signatures/active/db

*************************************************************
*  NEW INTRUSION SIGNATURES                                 *
*************************************************************

        /Trin00_Master-_Broadcast__msize__Command_-NG.db
        /Trin00_Master-_Broadcast__Password_144adsl__Seen_-NG.db
        /FTP_Client__STAT_File_Globbing__Attack_V1_-NG.db
        /Stacheldraht_Handler-_Agent_Probe_V2_-NG.db
        /NNTP_Client__AuthInfo_User_Overflow__Attack.db
        /HTTP_Client__MyWebServer_Search__Overflow_Attack_-NG.db
        /RedHat_Interchange_Server_Directory_Traversal_Attempt_-NG.db
        /SMTP_Client__HELO_Overflow__Attack_-NG.db
        /HTTP_Client__calendar.php_Command_Execution__Attack_-NG.db
        /HTTP_Client__Apache_2.0_Directory_Traversal_Execute__Attack -NG.db
        /Port[illegible]er__Du[illegible]ommand[illegible].db
```

Figure 3-42 Signature Upgrade Report (Upgrade Details)

In addition to the software versions and list of signatures, the Upgrade Details report displays upgrade path information and signature descriptions (see Figure 3-43).



```
*************************************************************
*  UNIQUE USER SIGNATURES                                   *
*************************************************************


       None.

*************************************************************
*  MERGED SIGNATURES                                        *
*  Note: The following marks provide detailed information:  *
*        '*' Indicates the preferred source of a field.     *
*        '+' Indicates a field added by User of Vendor.     *
*        '-' Indicates a field removed by User of Vendor.   *
*************************************************************

/Malformed_UDP_Packet_Fragment.db
        Original:       description =
                        Name: Malformed UDP Packet Fragment
                        Class: Protocol Anomaly
                        Decoder:
                        To enable this signature, the following decoder(s) must also be enabled:
                        IP Fragment Decoder
                        Description:
                        User Datagram Protocol (UDP) is a protocol standard within the TCP/IP protocol
                        suite that is used in place of TCP when reliable delivery is not required.
                        Packets that are larger than the maximum transmission unit of the underlying
                        layer  (for ethernet, this MTU is typically 1500) are fragmented into smaller
                        packets, which are then reassembled at the destination.
                        Some TCP/IP stack implementations suffer from a problem related to how the
                        TCP/IP stack handles reassembly of fragmented IP packets.  A malicious user
                        may attempt to exploit this type of flaw by custom crafting packets where
                        packet reassembly results in the data of one packet fragment overlapping
                        into the header of the previous fragment.
                        This signature detects packet fragments where the fragment offset is greater
```

Figure 3-43 Signature Upgrade Report (Signature Descriptions)

Chapter 4

Monitoring the SecureNet Sensor

This chapter provides the procedures for using the Intrusion SecureNet WBI to monitor the events detected by your SecureNet Sensor.

The procedures in this chapter can be randomly accessed. If you are reading this guide on hardcopy, use the Table of Contents to help you locate the procedure you want to perform. If you are reading this guide using a PDF reader, you can use the Table of Contents, use the search capabilities of the PDF reader, or use the PDF bookmarks in the reader's Navigation pane to find topics of interest.

Monitoring Options

The Monitoring menu (see Figure 4-1) lets you view the Event counts which show the number of events by signature, and create printable views of events.

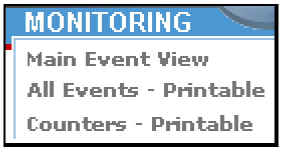


Figure 4-1 Events Menu

Procedures for each of these menu items are provided in the following sections:

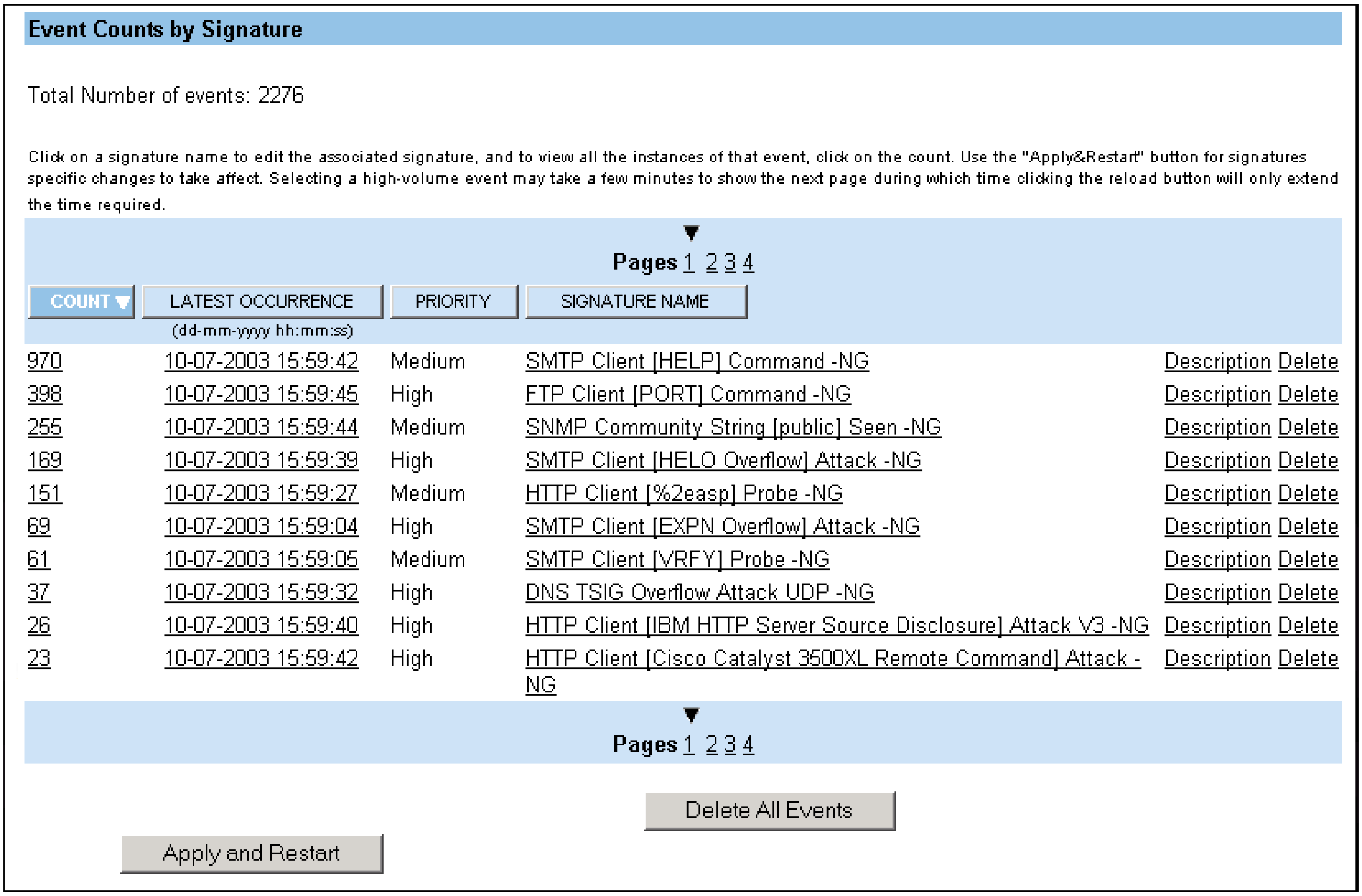
- "View Main Event View" on page 4-2
  - – "View Event Counts" on page 4-3
  - – "View Event Details" on page 4-4
  - – "Delete a Single Occurrence of an Event" on page 4-5
  - – "Delete an Event Group" on page 4-5
  - – "Delete All Event Groups" on page 4-5
  - – "Edit a Signature" on page 4-5
  - – "View a Signature's Description" on page 4-7
- "Print All Attacks with Counts" on page 4-10.
- "Print All Events with Source and Destination IP Addresses" on page 4-9.

View Main Event View

The main event view is the Event Counts by Signature page. To view this page, perform the following steps:

Step 1 From any Intrusion SecureNet WBI page, choose **Monitoring>Main Event View**.

The Event Counts by Signature page displays (see Figure 4-2).



Event Counts by Signature

Total Number of events: 2276

Click on a signature name to edit the associated signature, and to view all the instances of that event, click on the count. Use the "Apply&Restart" button for signatures specific changes to take affect. Selecting a high-volume event may take a few minutes to show the next page during which time clicking the reload button will only extend the time required.

Pages 1 2 3 4

COUNT ▼	LATEST OCCURRENCE (dd-mm-yyyy hh:mm:ss)	PRIORITY	SIGNATURE NAME	
970	10-07-2003 15:59:42	Medium	SMTP Client [HELP] Command -NG	Description Delete
398	10-07-2003 15:59:45	High	FTP Client [PORT] Command -NG	Description Delete
255	10-07-2003 15:59:44	Medium	SNMP Community String [public] Seen -NG	Description Delete
169	10-07-2003 15:59:39	High	SMTP Client [HELO Overflow] Attack -NG	Description Delete
151	10-07-2003 15:59:27	Medium	HTTP Client [%2easp] Probe -NG	Description Delete
69	10-07-2003 15:59:04	High	SMTP Client [EXPN Overflow] Attack -NG	Description Delete
61	10-07-2003 15:59:05	Medium	SMTP Client [VRFY] Probe -NG	Description Delete
37	10-07-2003 15:59:32	High	DNS TSIG Overflow Attack UDP -NG	Description Delete
26	10-07-2003 15:59:40	High	HTTP Client [IBM HTTP Server Source Disclosure] Attack V3 -NG	Description Delete
23	10-07-2003 15:59:42	High	HTTP Client [Cisco Catalyst 3500XL Remote Command] Attack -NG	Description Delete

Pages 1 2 3 4

Figure 4-2 Event Counts by Signature Page

The Event Counts by Signature page shows the total number of events at the top, and includes a table of the signatures that have the highest number of event counts.

Note The maximum number of lines displayed is user configurable. Refer to "Configure Intrusion SecureNet WBI Monitoring" on page 3-43. When the number of signatures exceeds the specified maximum number of lines per page, additional signatures are available to be displayed by clicking on the links at the top and bottom of the page.

The headers at the top of each column in the table can be used to sort the contents. You can click on a header to sort the events by that parameter. An arrow displays in the selected header to indicate the direction of the sort (top-down or bottom-up). Clicking on the same header again reverses the sorting direction.

The sections that follow explain how to view signature descriptions, to view event details, and to delete signatures and events.

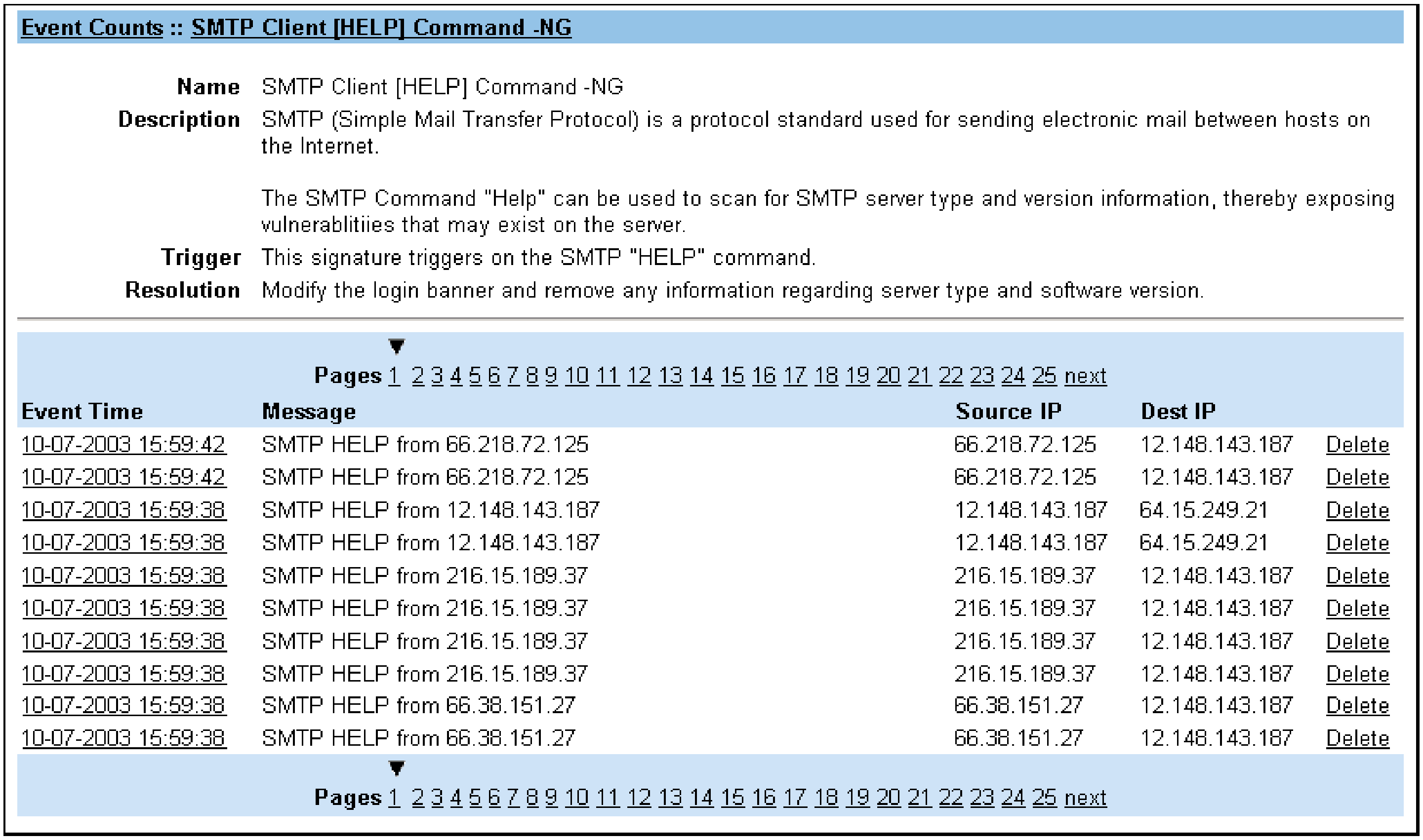
View Event Counts

To view the Event Counts for a selected signature, perform the following steps:

Step 1 If necessary, choose **Monitoring>Main Event View** from any Intrusion SecureNet WBI page to display the Event Counts by Signature page (see Figure 4-2).

Step 2 In the Signature Name column of the table, click on the event count of the signature for which you want to view the events.

The Event Counts page displays (see Figure 4-3).



Event Counts :: SMTP Client [HELP] Command -NG

Name SMTP Client [HELP] Command -NG

Description SMTP (Simple Mail Transfer Protocol) is a protocol standard used for sending electronic mail between hosts on the Internet.

The SMTP Command "Help" can be used to scan for SMTP server type and version information, thereby exposing vulnerablitiies that may exist on the server.

Trigger This signature triggers on the SMTP "HELP" command.

Resolution Modify the login banner and remove any information regarding server type and software version.

Pages 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 next

Event Time	Message	Source IP	Dest IP	
10-07-2003 15:59:42	SMTP HELP from 66.218.72.125	66.218.72.125	12.148.143.187	Delete
10-07-2003 15:59:42	SMTP HELP from 66.218.72.125	66.218.72.125	12.148.143.187	Delete
10-07-2003 15:59:38	SMTP HELP from 12.148.143.187	12.148.143.187	64.15.249.21	Delete
10-07-2003 15:59:38	SMTP HELP from 12.148.143.187	12.148.143.187	64.15.249.21	Delete
10-07-2003 15:59:38	SMTP HELP from 216.15.189.37	216.15.189.37	12.148.143.187	Delete
10-07-2003 15:59:38	SMTP HELP from 216.15.189.37	216.15.189.37	12.148.143.187	Delete
10-07-2003 15:59:38	SMTP HELP from 216.15.189.37	216.15.189.37	12.148.143.187	Delete
10-07-2003 15:59:38	SMTP HELP from 216.15.189.37	216.15.189.37	12.148.143.187	Delete
10-07-2003 15:59:38	SMTP HELP from 66.38.151.27	66.38.151.27	12.148.143.187	Delete
10-07-2003 15:59:38	SMTP HELP from 66.38.151.27	66.38.151.27	12.148.143.187	Delete

Pages 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 next

Figure 4-3 Event Counts Page

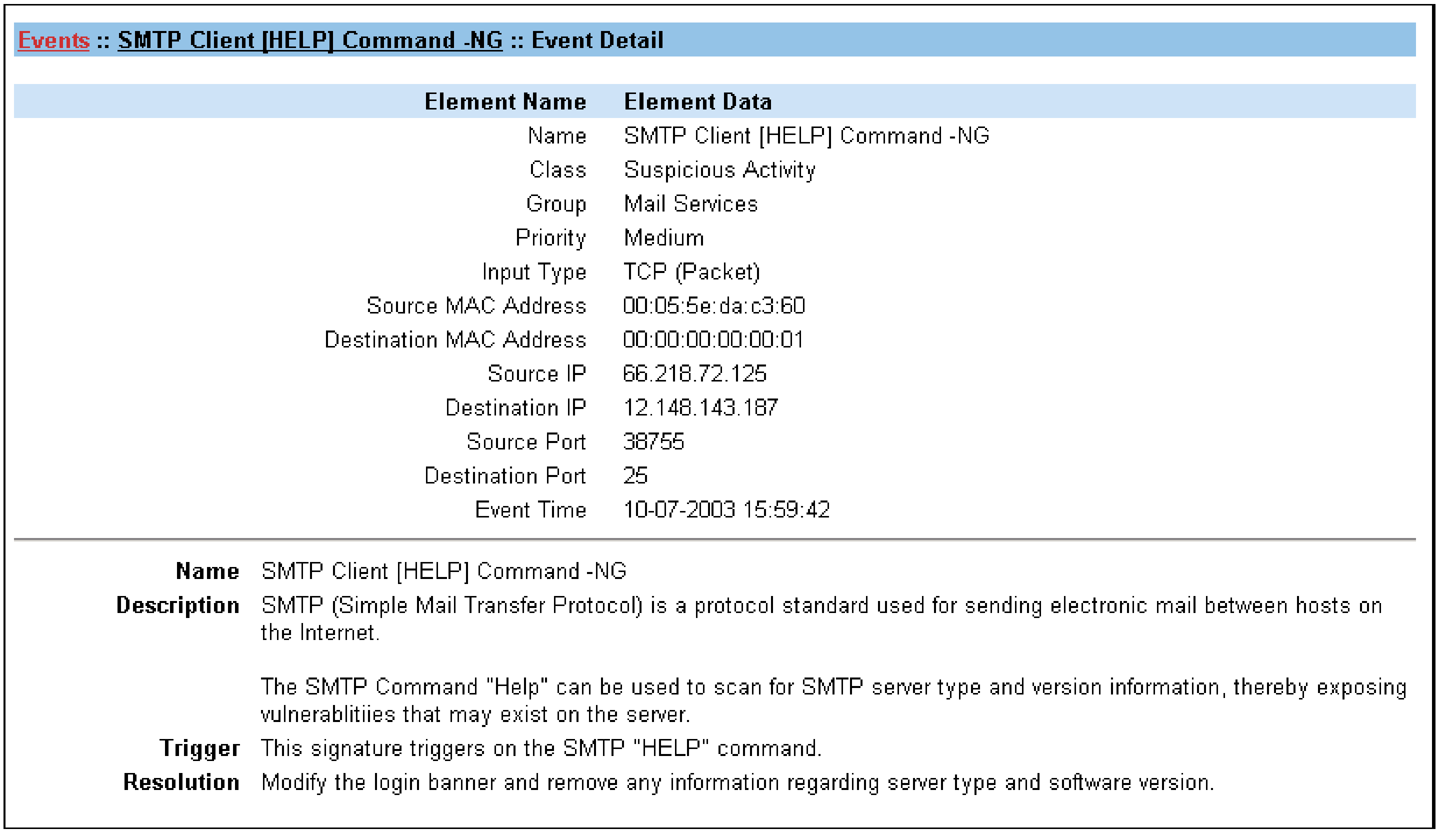
This page displays the individual events by Insertion Date (latest event first). The Message column contains the message created by the Sensor when the event was triggered. The Source IP and Dest IP columns display each event’s source IP address and Destination IP address, respectively.

This page also lets you view details of a selected event and it lets you delete any event that you no longer want to be in the list.

View Event Details

Step 1 To view the details for an event, go to the Event Counts page (see Figure 4-3) and click on the **Event Time** link (the link that appears in the **Event Time** column).

The Event Detail page for the selected event displays (see Figure 4-4).



Events :: SMTP Client [HELP] Command -NG :: Event Detail

Element Name	Element Data
Name	SMTP Client [HELP] Command -NG
Class	Suspicious Activity
Group	Mail Services
Priority	Medium
Input Type	TCP (Packet)
Source MAC Address	00:05:5e:da:c3:60
Destination MAC Address	00:00:00:00:00:01
Source IP	66.218.72.125
Destination IP	12.148.143.187
Source Port	38755
Destination Port	25
Event Time	10-07-2003 15:59:42

Name SMTP Client [HELP] Command -NG

Description SMTP (Simple Mail Transfer Protocol) is a protocol standard used for sending electronic mail between hosts on the Internet.

The SMTP Command "Help" can be used to scan for SMTP server type and version information, thereby exposing vulnerablitiies that may exist on the server.

Trigger This signature triggers on the SMTP "HELP" command.

Resolution Modify the login banner and remove any information regarding server type and software version.

Figure 4-4 Event Detail Page

Step 2 To return to the Events page, click on the **Events** link.

Delete a Single Occurrence of an Event

To delete a single occurrence of an event, perform the following steps:

Step 1 Go to the Events page (see Figure 4-3) and click on the **Delete** link to the right of the event occurrence that you want to delete.

The event is deleted.

Delete an Event Group

To delete an event group (all occurrences of a selected event), perform the following steps:

Step 1 Go to the Event Counts by Signature page (see Figure 4-2).

Step 2 Click on the **Delete** link to the right of the event group that you want to delete.

The event group is deleted.

Delete All Event Groups

To delete all event groups, perform the following steps:

Step 1 Go to the Event Counts by Signature page (see Figure 4-2).

Step 2 Click on the **Delete All Events** button at the bottom of the page.

All the Events are deleted.

Edit a Signature

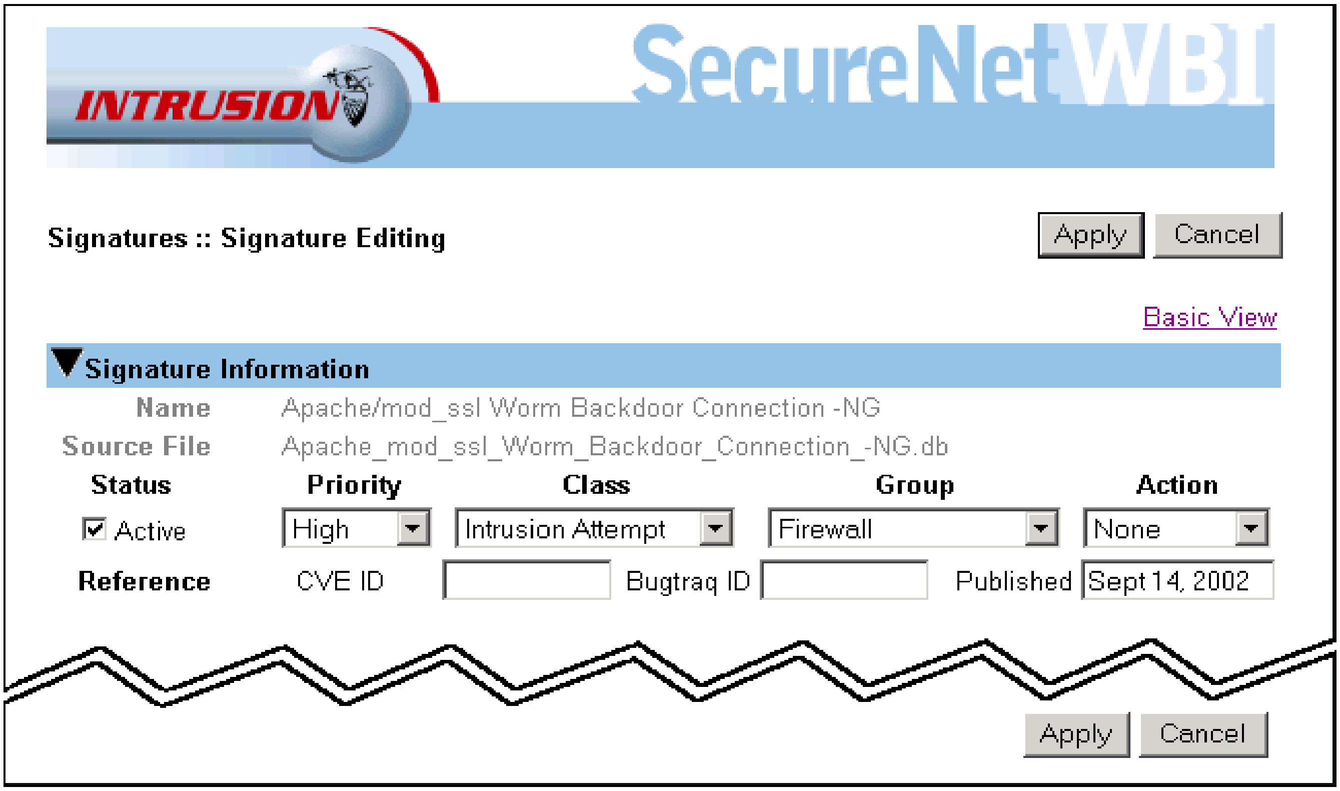
To edit a signature, perform the following steps:

Step 1 On the Event Counts by Signature page (see Figure 4-2), navigate to the location where the signature of interest is listed.

Note If you do not have Signature editing access, your Event Counts by Signature page will not display signature names as links because you are not allowed to edit signatures.

Step 2 Click on the signature’s name link in the **Signature Name** column of the table.

The Signature Editing page for that signature displays in a new window (see Figure 4-5).



Signatures :: Signature Editing

▼ Signature Information

Name Apache/mod_ssl Worm Backdoor Connection -NG

Source File Apache_mod_ssl_Worm_Backdoor_Connection_-NG.db

Status	Priority	Class	Group	Action
☑ Active	High	Intrusion Attempt	Firewall	None

Reference CVE ID Bugtraq ID Published Sept 14, 2002

Figure 4-5 Signature Editing Page (Signature Information)

Step 3 Refer to "Edit a Signature" on page 3-52 for instructions.

View a Signature's Description

There are two ways of viewing a signature's description: using a "mouse-over" action to view a brief description (only the narrative description) and clicking on a link to open a new window with a full, detailed description.

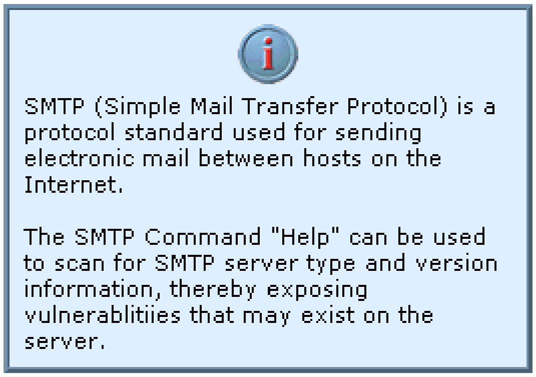
Get a Brief Description

To view the description for a specific signature, perform the following steps:

Step 1 On the Event Counts by Signature page (see Figure 4-2), navigate to the location where the signature of interest is listed.

Step 2 Move your mouse pointer over its **Description** link in the table.

The signature's description page displays in a popup window (see Figure 4-6).



SMTP (Simple Mail Transfer Protocol) is a protocol standard used for sending electronic mail between hosts on the Internet.

The SMTP Command "Help" can be used to scan for SMTP server type and version information, thereby exposing vulnerablitiies that may exist on the server.

Figure 4-6 Signature Description Popup Window

This window displays a brief description for the event. The contents vary according to the type of event being shown.

Step 3 After viewing the popup window, close it by moving your mouse pointer so that it is not over the Description link.

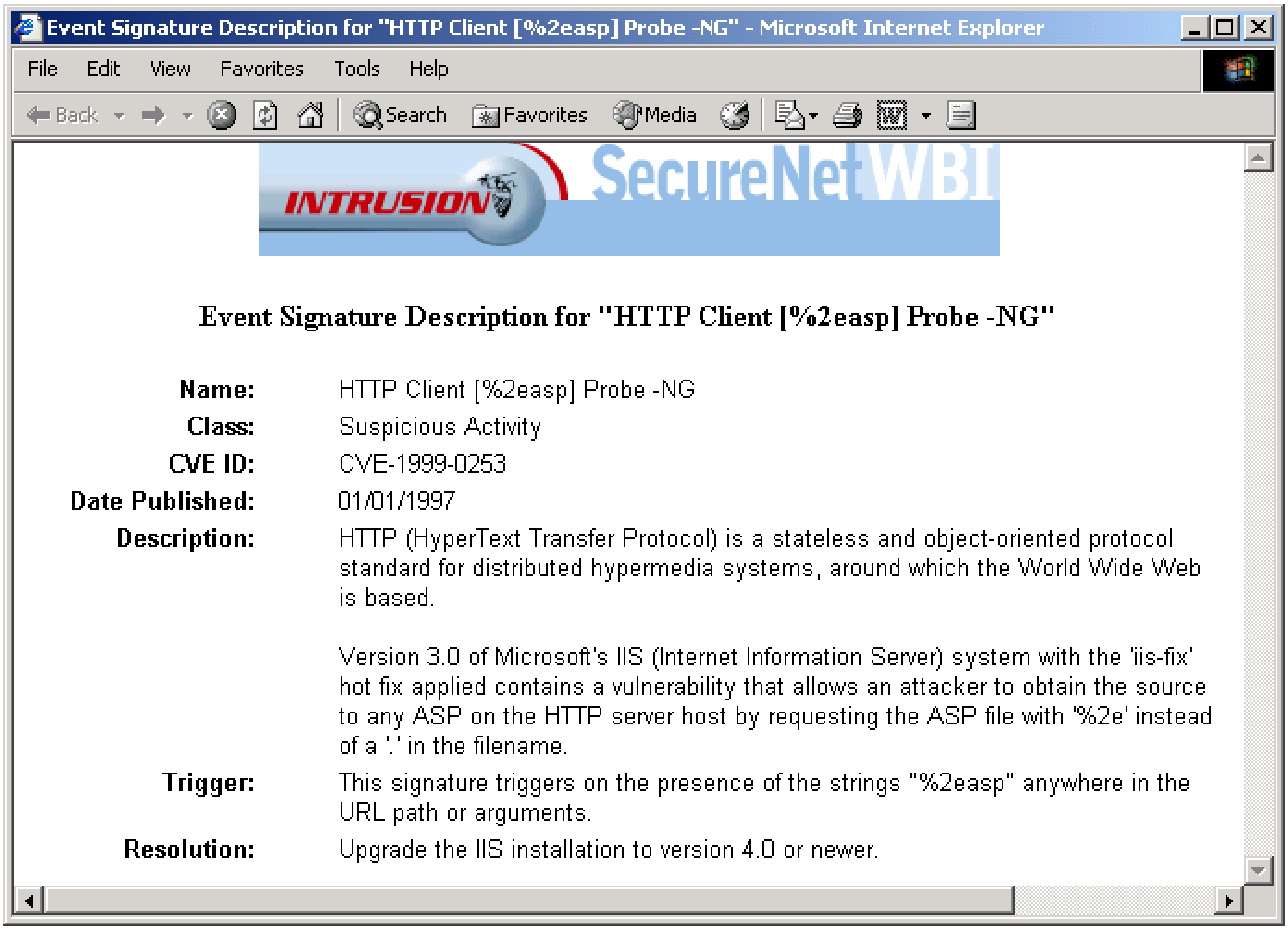
Get a Detailed Description

To view a more detailed description for a specific signature, pereform the following steps:

Step 1 On the Event Counts by Signature page (see Figure 4-2), navigate to the location where the signature of interest is listed.

Step 2 Click on its **Description** link in the table.

The signature's description page displays in a new window (see Figure 4-7).


Event Signature Description for "HTTP Client [%2easp] Probe -NG" - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
INTRUSION
SecureNet WBI

Event Signature Description for "HTTP Client [%2easp] Probe -NG"

Name: HTTP Client [%2easp] Probe -NG

Class: Suspicious Activity

CVE ID: CVE-1999-0253

Date Published: 01/01/1997

Description: HTTP (HyperText Transfer Protocol) is a stateless and object-oriented protocol standard for distributed hypermedia systems, around which the World Wide Web is based.

Version 3.0 of Microsoft's IIS (Internet Information Server) system with the 'iis-fix' hot fix applied contains a vulnerability that allows an attacker to obtain the source to any ASP on the HTTP server host by requesting the ASP file with '%2e' instead of a '.' in the filename.

Trigger: This signature triggers on the presence of the strings "%2easp" anywhere in the URL path or arguments.

Resolution: Upgrade the IIS installation to version 4.0 or newer.

Figure 4-7 Signature Description Window

This window displays the details for the event. The contents vary according to the type of event being shown.

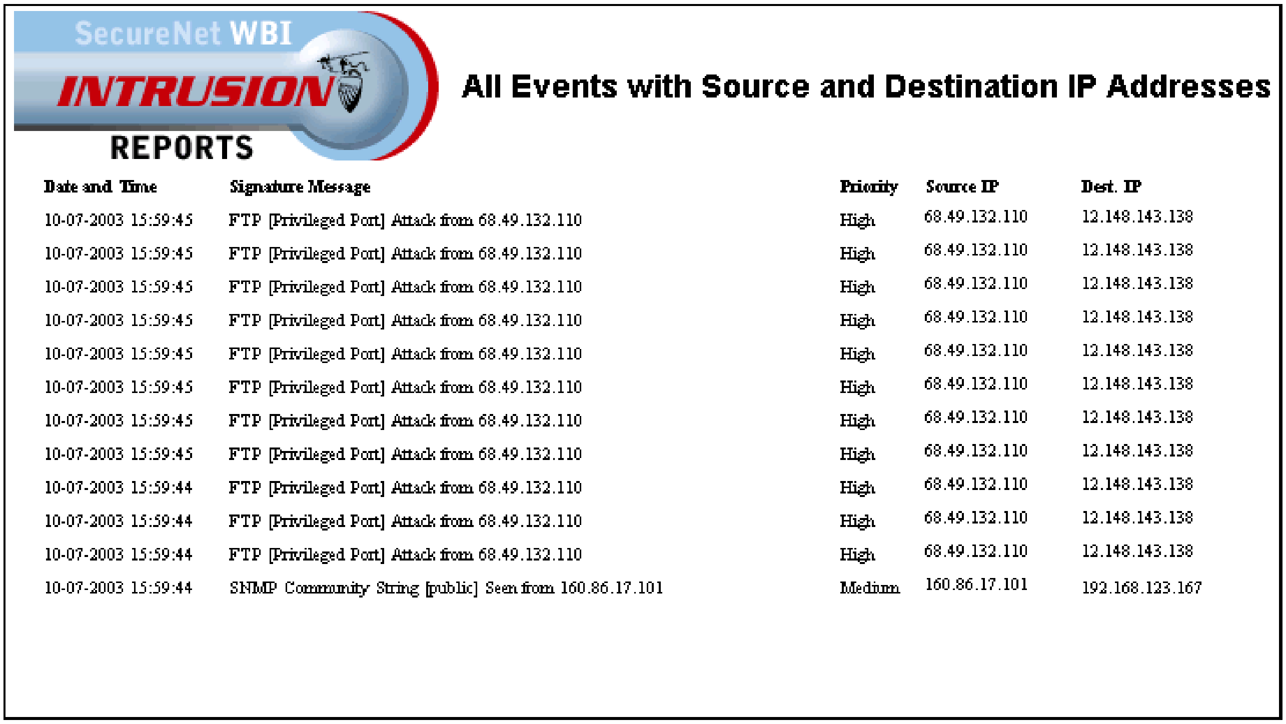
Step 3 After viewing the window, close it by clicking on the close box in the upper right corner of the window.

Print All Events with Source and Destination IP Addresses

To print a list of all events with their Source and Destination IP addresses, perform the following steps:

Step 1 From any Intrusion SecureNet WBI page (see Figure 4-1), choose **Monitoring>All Events - Printable**.

The All Events with Source and Destination Addresses - Printable page displays (see Figure 4-8).



All Events with Source and Destination IP Addresses

Date and Time	Signature Message	Priority	Source IP	Dest. IP
10-07-2003 15:59:45	FTP [Privileged Port] Attack from 68.49.132.110	High	68.49.132.110	12.148.143.138
10-07-2003 15:59:45	FTP [Privileged Port] Attack from 68.49.132.110	High	68.49.132.110	12.148.143.138
10-07-2003 15:59:45	FTP [Privileged Port] Attack from 68.49.132.110	High	68.49.132.110	12.148.143.138
10-07-2003 15:59:45	FTP [Privileged Port] Attack from 68.49.132.110	High	68.49.132.110	12.148.143.138
10-07-2003 15:59:45	FTP [Privileged Port] Attack from 68.49.132.110	High	68.49.132.110	12.148.143.138
10-07-2003 15:59:45	FTP [Privileged Port] Attack from 68.49.132.110	High	68.49.132.110	12.148.143.138
10-07-2003 15:59:45	FTP [Privileged Port] Attack from 68.49.132.110	High	68.49.132.110	12.148.143.138
10-07-2003 15:59:45	FTP [Privileged Port] Attack from 68.49.132.110	High	68.49.132.110	12.148.143.138
10-07-2003 15:59:44	FTP [Privileged Port] Attack from 68.49.132.110	High	68.49.132.110	12.148.143.138
10-07-2003 15:59:44	FTP [Privileged Port] Attack from 68.49.132.110	High	68.49.132.110	12.148.143.138
10-07-2003 15:59:44	FTP [Privileged Port] Attack from 68.49.132.110	High	68.49.132.110	12.148.143.138
10-07-2003 15:59:44	SNMP Community String [public] Seen from 160.86.17.101	Medium	160.86.17.101	192.168.123.167

Figure 4-8 All Events with Source and Destination IP Addresses - Printable Page

Note If there are a large number of events, it may take a while for the window to open. Be patient and wait for it to completely display.

Step 2 On the browser window, choose **File>Print**.

A Windows Print dialog displays.

Step 3 In the Print dialog, choose the printer on which you want to print the events and then set the paper orientation to **Portrait**.

Step 4 Set any other print options you want and then click on **Print**.

The selected page is printed.

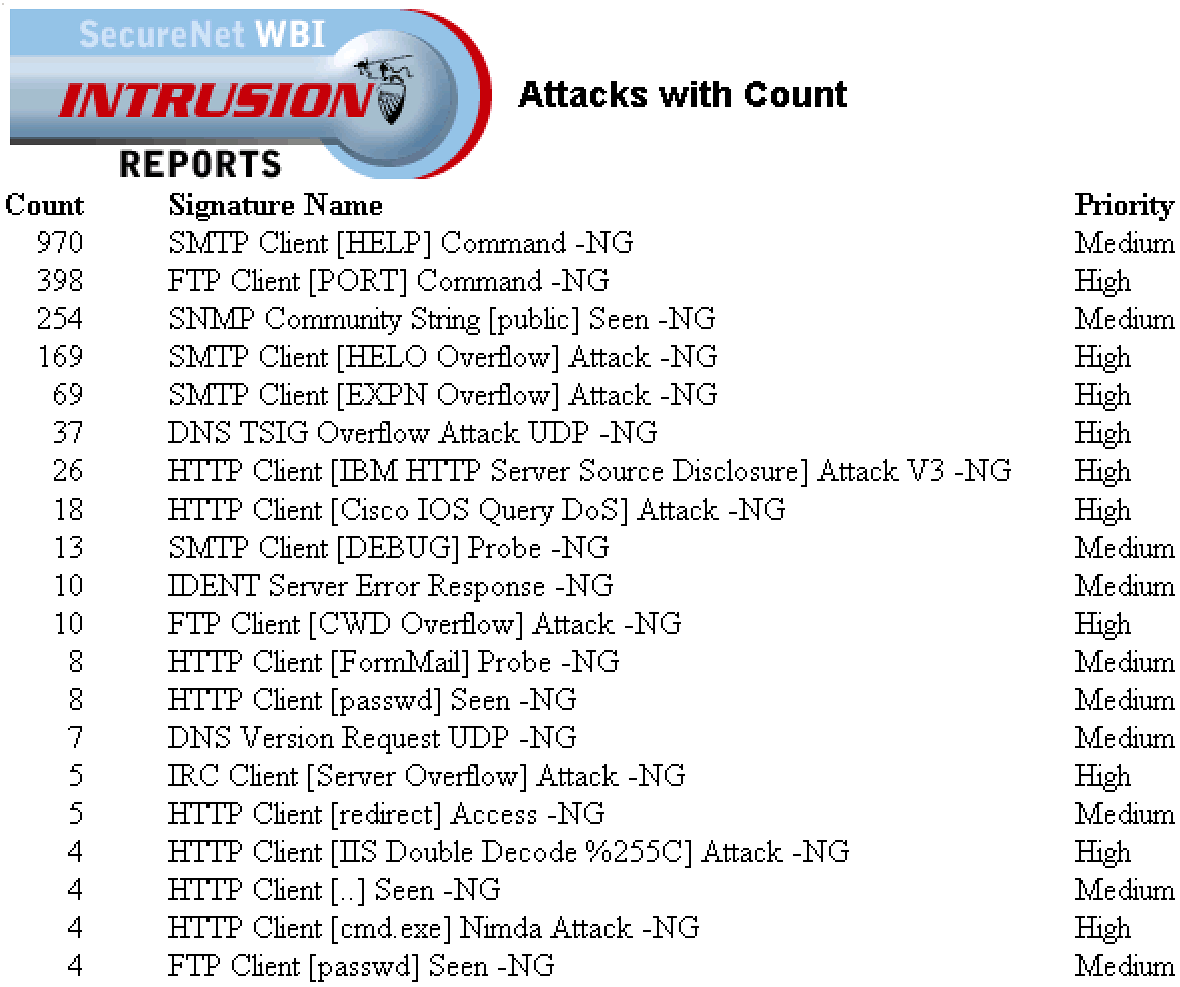
Step 5 Close the browser window.

Print All Attacks with Counts

To print a list of all attack signatures that have at least one event listed by the highest number of events counted down to the lowest number of events counted, perform the following steps:

Step 1 From any Intrusion SecureNet WBI page (see Figure 4-1), choose **Monitoring>Counts - Printable**.

The Attacks with Count - Printable page displays (see Figure 4-9)



Attacks with Count

Count	Signature Name	Priority
970	SMTP Client [HELP] Command -NG	Medium
398	FTP Client [PORT] Command -NG	High
254	SNMP Community String [public] Seen -NG	Medium
169	SMTP Client [HELO Overflow] Attack -NG	High
69	SMTP Client [EXPN Overflow] Attack -NG	High
37	DNS TSIG Overflow Attack UDP -NG	High
26	HTTP Client [IBM HTTP Server Source Disclosure] Attack V3 -NG	High
18	HTTP Client [Cisco IOS Query DoS] Attack -NG	High
13	SMTP Client [DEBUG] Probe -NG	Medium
10	IDENT Server Error Response -NG	Medium
10	FTP Client [CWD Overflow] Attack -NG	High
8	HTTP Client [FormMail] Probe -NG	Medium
8	HTTP Client [passwd] Seen -NG	Medium
7	DNS Version Request UDP -NG	Medium
5	IRC Client [Server Overflow] Attack -NG	High
5	HTTP Client [redirect] Access -NG	Medium
4	HTTP Client [IIS Double Decode %255C] Attack -NG	High
4	HTTP Client [..] Seen -NG	Medium
4	HTTP Client [cmd.exe] Nimda Attack -NG	High
4	FTP Client [passwd] Seen -NG	Medium

Figure 4-9 Attacks with Count - Printable Page

Note If there are a large number of attacks with counts, it may take a while for the window to open. Be patient and wait for it to completely display.

Step 2 On the browser window, choose **File>Print**.

A Windows Print dialog displays.

Step 3 In the Print dialog, choose the printer on which you want to print the events and then set the paper orientation to **Portrait**.

Step 4 Set any other print options you want and then click on **Print**.

The selected page is printed.

Step 5 Close the browser window.

Appendix A

Field Formatting and Event Filtering

This appendix provides information for formatting entries for fields and some details about the filtering capability for signatures.

Field Formatting

Action

This configuration option specifies the action that should be taken when a signature activates. Valid action values are listed below:

- Reset TCP Session
- Text log
- Binary log
- Do Nothing
- TCPdump Log

Note The Reset TCP option is available only when using the TCP Stream, TCP Any, or NULL input source.

Case-Sensitive

When the Case-Sensitive configuration option is enabled, it specifies that network grep strings should be searched for in a case sensitive manner.

Note The Case Sensitive option requires an entry in the String field.

Coalescing Count

This configuration option specifies the number of times a signature must be triggered before it engages in any logging or notification activities. Valid values are:

0 - 16383 - Number of triggers required before logging/notification

Coalescing Interval

This configuration option specifies a timeout period (in seconds) after a signature triggers that it will not trigger again.

Valid values are 0 - 16383

Compact Spaces

When enabled, the **Compact Spaces** configuration option specifies whether whitespace (tabs or spaces) between individual extracted network grep arguments should be compacted into a single character of whitespace.

Email

The **Email** configuration option specifies an electronic mail address to which signature activation notification should be sent. Notification is sent only if a ‘Message:’ configuration parameter is configured.

The format of this parameter is *user@host.*

Note This option will be used only if email notification is globally configured on the Sensor host.

Group

This configuration option specifies the classification group of the signature.

Currently Intrusion Inc. uses the following 12 groups, though any custom group can be added and used:

- DNS Services
- Firewall Services
- FTP Services
- Host Services
- IDS Services - reserved for decoder signatures
- Instant Messaging Services
- Mail Services
- Network Information Services
- News Services
- Remote Access Services
- Router Services
- Web Services

ICMP Code

This configuration option filters on ICMP code. Option valid in SecureNet Sensor versions 4.4 and newer.

Valid values are 0 - 15.

Note This configuration option is available only when using the ICMP input source.

ICMP EchoID

This configuration option filters on ICMP echo ID number. The ICMP type must equal 0. Option valid in SecureNet Sensor version 4.4 and later.

Valid values are non-negative integers less than 16383.

Note This configuration option is available only when using the ICMP input Source.

ICMP EchoSeq

This configuration option filters on ICMP echo sequence number. The ICMP type must equal 0. Option valid in SecureNet Sensor versions 4.4 and newer.

Valid values are non-negative integers less than 16383.

Note This configuration option is available only when using the ICMP input source.

ICMP Type

This configuration option filters on ICMP message type. Option valid in SecureNet Sensor versions 4.4 and newer.

Valid values are 0 - 32767.

Note This configuration option is available only when using the ICMP input source.

Input Source

This configuration option specifies the input protocol or trigger type that results in the signature being evaluated. Valid input type values are:

- TCP Stream
- TCP Packet
- UDP Packet
- ICMP Packet
- IP Packet
- Ether Packet
- Raw Packet
- Null
- IGMP
- IP Fragment

- TCP Any- provides TCP Stream if available (that is if TCP reassembly is turned on in the sensor) otherwise it provides TCP Packet
- HTTP- provides HTTP normalized URL packets when URL normalization is turned on (in the sensor) otherwise it provides raw TCP Packets

IP Address

This configuration options specify source and destination IP filtering parameters for a signature.

Note These filtering options are not available when using Raw Packet or Ether Packet as the input source type.

The IP address formatting is as follows:

*	Wildcard (Type the asterisk to indicate any valid number for part of the address. Wildcards can be used in addresses and ranges.)
+ (Include) or - (Exclude)	The plus sign ('+') indicates inclusion and the minus sign ('-') indicates exclusion. Exclusion and inclusion of addresses can be mixed.
x.x.x.x	Specific IP address, where *x* can be any value from 0 to 255.
x.x.x.*	IP class range. One or more of the parts of an address may be specified as a wildcard
x.x.x.x - x	IP address range. One or more of the fields in an address may be specified as a range.
x.x.x.x, x.x.x-x.x or +x.x.x.x,+x.*.x.x,+x.x-x.x.x or -x.x.x.x, -x.x.x.*, -x.x.x-x.x-x	List of comma-delimited IP addresses or addresses and ranges. The range can include wildcard characters and the inclusion ('+') and exclusion ('-')characters.

Examples:

a. Include a single IP address 1.1.1.1 and exclude all other IP addresses:

   +1.1.1.1

b. Exclude a single IP address 1.1.1.1 and include all other IP addresses:

   -1.1.1.1

c. Include all IP addresses for the C-class and exclude all other IP addresses:

   +1.1.1.* Or **+1.1.1.0-255**

d. Exclude all IP addresses from C-class and include all other IP addresses:

   -1.1.1.* Or **-1.1.1.0-255**

e. Include list of IP addresses and exclude all other IP addresses:

+1.1.1.1, +2.2.2.2, +3.3.3.3

f. Exclude list of IP addresses and include all other IP addresses:

-1.1.1.1, -2.2.2.2, -3.3.3.3

g. Excluding and including IP addresses in a list will result in the inclusion of each address for which inclusion is indicated and the exclusion of all other IP addresses. For example, the following line of rules for inclusion and exclusion:

-1.1.1.1, +2.2.2.2, +3.3.3.3, -4.4.4.4

causes signatures to behave identically to the following rule:

+2.2.2.2, +3.3.3.3

With the following rule:

+1.1.1.*, -1.1.1.1,

A packet with IP 1.1.1.1 will be allowed because it is specifically included in the first rule, and the second rule would not be evaluated.

-1.1.1.1, +1.1.1.*

However, with this rule a packet with IP 1.1.1.1 will **not** be allowed since it is first excluded; the second inclusionary rule will not be evaluated. Only packets that pass the +1.1.1.* rule will be allowed.

IP Pairs

This configuration option specifies source and destination IP address filtering parameters for a signature.

Note These filtering options are not available when using Raw Packet or Ether Packet as the input source type.

The IP Pair must include valid source and destination IP addresses with an '@' symbol between, in the format:

<sourceIP>, *<sourceIP>*, *<sourceIP>*@*<destinationIP>*, *<destinationIP>*,*<destinationIP>*

where *sourceIP* and *destinationIP* can use the following format:

*	Wildcard (Type the asterisk to indicate any valid number for a position. Wildcards can be used in addresses and ranges.)
x.x.x.x	Specific IP address, where *x* can be any value from 0 to 255.
x.x.x.*	IP class range. One or more of the fields in an address may be specified as a wildcard

x.x.x.x - x	IP address range. One or more of the fields in an address may be specified as a range.
x.x.x.x, x.x.x-x.x or x.x.x.x +x.*.x.x, +x.x-x.x.x or -x.x.x.x, -x.x.x.*, -x.x.x-x.x-x	List of comma-delimited IP addresses or addresses and ranges. The range can include wildcard characters and the inclusion (‘+’) and exclusion (‘-’)characters.

Examples:

a. Include a single IP-Pair source 1.1.1.1 and destination 2.2.2.2:

+1.1.1.1@+2.2.2.2

b. Exclude a single IP-Pair source 1.1.1.1 and destination 2.2.2.2

-1.1.1.1@-2.2.2.2

c. Include all IP-Pairs from source C-class 1.1.1 and destination 2.2.2.2

+1.1.1.*@+2.2.2.2

Or

+1.1.1.0-255@+2.2.2.2

d. Exclude all IP-Pairs from source C-class 1.1.1 and destination 2.2.2.2

-1.1.1.*@-2.2.2.2

Or

-1.1.1.0-255@-2.2.2.2

e. Include a list of IP-Pairs with source 1.1.1.1, 3.3.3.3, 5.5.5.5 and destination 2.2.2.2, 4.4.4.4, 6.6.6.6

+1.1.1.1, +2.2.2.2, +3.3.3.3 @ +4.4.4.4, +5.5.5.5, +6.6.6.6

f. Exclude list of IP-Pairs with source 1.1.1.1, 3.3.3.3, 5.5.5.5 and destination 2.2.2.2, 4.4.4.4, 6.6.6.6

-1.1.1.1, -2.2.2.2, -3.3.3.3 @ -4.4.4.4, -5.5.5.5, -6.6.6.6

g. Exclude and include list of IP-Pairs with source 1.1.1.1, 3.3.3.3, 5.5.5.5 and destination 2.2.2.2, 4.4.4.4, 6.6.6.6

-1.1.1.1, +3.3.3.3, -5.5.5.5 @ +2.2.2.2, +4.4.4.4, -6.6.6.6

this rule above is identical to the following rule:

+3.3.3.3 @ +2.2.2.2, +4.4.4.4

Consider the following rule:

+4.4.4.* @ +5.5.5.5

This rule will allow packets with IP source addresses of 4.4.4.4, 4.4.4.10, and 4.4.4.255 only if the destination IP is 5.5.5.5. However, the rule will not allow addresses 4.4.4.4, 4.4.4.10 and 4.4.4.255 if the destination IP is 1.1.1.1.

Conversely, if the destination IP address for a packet is 5.5.5.5 the rule would allow the packet only if the source IP address is 4.4.4.4, 4.4.4.10, or 4.4.4.255, but would not allow the packet if the source IP is 1.1.1.1.

MAC Address

This configuration options specify source and destination MAC address filtering parameters for a signature.

Note These filtering options are not available when using the Raw Packet input source type.

Filtering values may be formatted as follows:

*	Wildcard (Type the asterisk to indicate any valid number for a position. Wildcards can be used in addresses and ranges.)
+ (Include) or - (Exclude)	The plus sign ('+') indicates inclusion and the minus sign ('-') indicates exclusion. Exclusion and inclusion of MAC addresses can be mixed.
xx:xx:xx:xx:xx:xx	Specific MAC address, where *xx* can be any value from 00 to FF.
xx:xx:xx:xx:*:xx	MAC address range. One or more of the positions in an address may be specified as a wildcard.
xx:xx:xx:xx:xx:xx-xx	MAC address range. One or more of the positions in an address may be specified as a range.
xx:xx:xx:xx:xx:xx, xx:xx:xx:xx:xx:xx or +xx:xx:xx:xx:xx:xx, -xx:xx:xx-xx:xx:xx, +xx:xx:xx:*:xx:xx	Comma-delimited IP address range. The range can include wildcard characters and the inclusion ('+') and exclusion ('-')characters.

Examples:

a. Include a single MAC address 11:11:11:11:11:11 and exclude all other MAC addresses

   +11:11:11:11:11:11

b. Exclude a single MAC address 11:11:11:11:11:11 and include all other MAC addresses

   -11:11:11:11:11:11

c. Include all MAC addresses in a range and exclude all other MAC addresses:

   +11:11:11:11:11:*

Or

+11:11:11:11:11:00-FF

d. Exclude all MAC addresses in a range and include all other MAC addresses:

-11:11:11:11:11:*

Or

-11:11:11:11:11:00-FF

e. Include list of MAC addresses and exclude all other MAC addresses:

+11:11:11:11:11:11, +22:22:22:22:22:22, +33:33:33:33:33:33

f. Exclude list of MAC addresses and exclude all other MAC addresses:

-11:11:11:11:11:11, -22:22:22:22:22:22, -33:33:33:33:33:33

g. Include and exclude MAC addresses in a list, will include all inclusionary MAC addresses and exclude all other MAC addresses:

-11:11:11:11:11:11, +22:22:22:22:22:22, -33:33:33:33:33:33

The rule above is identical to the following rule:

+22:22:22:22:22:22

Consider the following rule:

-11:11:11:11:11:*, +11:11:11:*:*:*

This rule includes all MAC addresses within the range of 11:11:11:*:*:*, with the exception of 11:11:11:11:11:*, which is excluded. All other MAC addresses are excluded.

Message

This configuration option specifies a message that will be logged to the event database. Messages are triggered upon the signature firing.

The message is a text string that can contain one or more of the following conversion specifiers. When the signature is triggered, these conversion specifiers are replaced with the context-specific data to which they correspond.

The following conversion specifiers are supported:

- **~SRCETHER**—Corresponds to the source Ethernet MAC address of the network activity that caused the signature to be triggered.
- **~DSTETHER**—Corresponds to the destination Ethernet MAC address of the network activity that caused the signature to be triggered.
- **~SRCIP**—Corresponds to the source IP address of the network activity that caused the signature to be triggered.
- **~DSTIP**—Corresponds to the destination IP address of the network activity that caused the signature to be triggered.
- **~SRCPORT**—Corresponds to the source TCP/UDP port of the network activity that caused the signature to be triggered.

- **~DSTPORT**—Corresponds to the destination TCP/UDP port of the network activity that caused the signature to be triggered.
- **~ARGDATA?**—Corresponds to a piece of data extracted from the TCP connection or individual packet that caused the signature to be triggered. The '?' character must be replaced with an appropriate argument number (0 - 6).
- **~SENSOR**—Corresponds to the Sensor that contained the signature which triggered.

Packet Coalescing

This configuration option specifies whether a signature may be triggered more than once on a single captured packet. Valid values are:

- On- Coalesce triggering, that is do not trigger multiple times on a single packet
- Off- Do not coalesce triggering, that is do not trigger multiple times on a single packet

Payload-ExactSz

This configuration option filters based on packet payload size. The payload must be exactly the same size as parameter to pass filter check. Option valid in SecureNet Sensor versions 4.4 and newer. The format of this parameter is a positive integer in Bytes.

Payload-MinSize

This configuration option filters based on packet payload size. The payload must be as large or larger than parameter to pass filter check. Option valid in SecureNet Sensor versions 4.4 and newer. The format of this parameter is a positive integer in bytes.

Port: (Source-Port, Dest-Port)

This configuration options specify source and destination UDP or TCP port filtering parameters for a signature.

Note These filtering options are available only when using the TCP, UDP, TCP Stream, TCP Any, HTTP, or NULL input sources.

Filtering values can be formatted as follows:

*	Wildcard
+ (Include) or - (Exclude)	Type the inclusion character ('+') to include a port or range of ports or type the exclusion character ('-') to exclude a port or range of ports.
x	Specific port, where *x* can be any value from 0 to 65535.
x-x	Port range
+x, +x-x, -x, -x-x	Comma-delimited list of port filtering options. A maximum of four options may be specified.

Examples:

a. Include a single Port 111, and exclude all other ports:

   +111

b. Exclude a single Port 111 and include all other ports:

   -111

c. Include all ports in a range and exclude all other ports:

   +111-1024

d. Exclude all ports in a range and include all other ports:

   -111-1024

e. Include list of ports and exclude all other ports:

   +111, +222, +333

f. Exclude list of ports and include all other ports:

   -111, -222, -333

g. Excluding and including ports in a list will result in the inclusion of all ports for which inclusion is indicated and the exclusion of all other ports:

   -111, +222, +333, -444

   Therefore, the example above will behave identically as with the following rule:

   +222, +333

   Consider the following rule:

   -100-500, +1-1024

   For this rule, all ports in the range 1-1024 are included except for packets in the range 100-500, which are excluded.

Priority

This configuration option specifies the signature priority. Valid priorities are:

- Low
- Med
- High

Same IP

When checked, this configuration option filters based on matching source and destination IP addresses. Packets containing the same source and destination IP will pass the filter check. Option valid in SecureNet Sensor versions 4.4 and newer.

Note This configuration option is not available when using the Raw Packet or Ether Packet input source type.

Same Ports

When checked, the Same-Ports configuration option filters based on matching source/destination TCP/UDP ports. Packets containing both the same source and destination port will pass filter check. Option valid in SecureNet Sensor versions 4.4 and newer.

Scan-End

This configuration option specifies the specific end of a TCP connection circuit that should be scanned for a network grep string. Valid values for this parameter are listed below:

- Client
- Server
- Both client and server

Note This option requires the use of the String option.

String

This configuration option specifies a network grep data scanning string that the signature configures the SecureNet Sensor to search for.

Note This configuration option is not available when using the Null input source.

In addition to being able to search for simple text strings, SecureNet Sensor's data scanning facilities can be used to perform a variety of complex data parsing and analysis tasks including:

- Multi-argument String Matching—SecureNet Sensor's data scanning facilities are capable of searching for multiple disjointed string arguments.
- Argument Extraction—Information lying between two positively identified data scanning strings can be extracted. This extracted data can be included in SecureNet Sensor messages and other useful information.
- Distance Between Strings Analysis—Analysis can be performed based on the distance between two positively identified data scanning strings, allowing for easy detection of buffer overflow attacks.

To use SecureNet Sensor's data-scanning to its fullest extent, you must understand how data scanning strings are formatted. By creating specially formatted data scanning strings, you can use SecureNet Sensor's advanced data scanning features, such as argument extraction. The format of data scanning strings is as follows:

```
<argument><separator><argument>...
```

Examples:

passwd

USER*256*\010

Arguments specify raw text strings to be searched for. They may contain standard printable characters or special characters. Special characters can be specified through the use of ASCII escape codes. These codes are formatted as follows:

```
\<ascii-code>
```

Examples:

\010

\013

\254

Separators mark the boundaries between two text arguments to be scanned for. You can also access extra functionality such as argument extraction or distance between strings analysis by using separators. Separators are formatted as follows:

```
*length-valueSEPARATOR-FLAG
```

Examples:

100

*0=

*2000>

The beginning of a separator is always marked using an asterisk '*' character.

This character may not be specified directly in a scanning argument. Instead, you must use the character escape code \042 in place of the asterisk.

The length-value parameter specifies a length value to be used when evaluating SEPARATOR_FLAG. The SEPARATOR_FLAG parameter is a single character that controls the type of data scanning operation that should occur when scanning between two argument boundaries. The SEPARATOR_FLAG characters that can be used are listed in Table A-1.

Table A-1 SEPARATOR FLAG Characters

Character	Description
*	Matches positively regardless of the number of bytes separating two identified strings. When the '*' SEPARATOR_FLAG is used, the length-value parameter has no effect, other than specifying a maximum number of characters that can be extracted for usage in event messages.
=	Matches positively only if the number of bytes separating two identified strings is equal to the length-value parameter.

Table A-1 SEPARATOR FLAG Characters- **(Continued)**

Character	Description
>	Matches positively only if the number of bytes separating two identified strings is greater than the length-value parameter.
<	Matches positively only if the number of bytes separating the two identified strings is less than the length-value parameter.

When specifying multi-argument data scanning strings, you can include up to six separate text arguments. A separator must be placed between each argument, otherwise the scanning string will be evaluated as a single argument. By using separators in combination with multi-argument strings, you can perform complex data parsing tasks easily.

This configuration option filters based on TCP flag (FIN, SYN, RST, PSH, ACK, URG, ECN, and CWR respectively). Option valid in SecureNet Sensor versions 4.4 and newer.

Valid values are:

- **Yes**- Flag must be set.
- **NA** - Don't care.
- **No**- Flag must not be set.

Note This configuration option is available only when using the TCP Packet input source.

Event Filtering

Intrusion SecureNet WBI allows you to perform some editing of signatures. Changes you make for signatures can include the specification of filtering for events (including or excluding potential sources of noisy events) for a signature. By specifying certain MAC addresses, IP addresses, ports, IP-pairs, or ranges of same, you can customize signatures and reduce the number of events that must be analyzed.

Event Filtering Rules

When event filtering is specified to affect how signatures will be triggered, the following rules apply:

- **No filtering:** If no filter is specified the signature will trigger an event, when appropriate, regardless of the IP addresses, MAC addresses, and/or Ports.
- **Exclusionary filtering only:** If a filter does exist and all rules in the filter are exclusionary rules (that is, they exclude IP addresses, MAC addresses, or ports), then the signature will not trigger an event for the IP address, MAC address or Port values that are specifically excluded.

  For example, a rule that excludes A and B ("-A, -B") **would not** trigger an event if the packet had A or B, but **would** trigger an event if the packet had C.
- **Inclusionary filtering only:** If a filter does exist and all rules in the filter are inclusionary rules (that is, they include IP addresses, MAC addresses or ports), then the signature will trigger an event, when appropriate, only if the IP address, MAC address or port is explicitly included.

  For example, a rules that includes A and B ("+A, +B") **would** trigger an event if the packet had A or B, but **would not** trigger an event if the packet had C.
- **Combination of inclusionary and exclusionary filtering**: If a filter does exist and it has rules that are both inclusionary as well as exclusionary (that is, they include or exclude IP addresses, MAC addresses or ports), then the signature will trigger an event, when appropriate, only if the IP address, MAC address, or port is explicitly included in one or more of the inclusionary rules (unless the packet was also excluded in an earlier rule). If a packet matches against an exclusionary rule, the signature will not trigger an event on it even if an inclusion rule exists later in the filter. The inclusion/exclusion rules are evaluated from left to right, and rule evaluation ends on the first rule match.

  For example, the rule "-B, +A-F" that excludes B but includes a range A-F, which contains B, **would not t**rigger an event if the packet had B, since the exclusionary rule matched first, the inclusionary rule is not evaluated. This rule **would** also trigger an event if the packet had A, C, D, E, or F, but not if the packet had G since it is not specifically included. However, the rule "+A-F, -B" that includes a range A-F, which contains B, and then excludes B **would** trigger an event if the packet had B since the inclusionary rule would match first, the exclusionary rule would not be evaluated. This rule **would not** trigger an event if the packet had G, because G is not specifically included.